# P-660H-T1v3s

*ADSL2+ 4-port Gateway*

# User's Guide

## Default Login Details

| | |
|---|---|
| IP Address | http://192.168.1.1 |
| Password | 1234 |

Firmware Version 3.12
Edition 2, 6/2010

**www.zyxel.com**

ZyXEL

Copyright © 2010
ZyXEL Communications Corporation

# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the P-660H-T1v3s using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

## Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

Note: It is recommended you use the web configurator to configure the P-660H-T1v3s.

- Support Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

## User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

## Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

## Disclaimer

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

**Warnings tell you about things that could harm you or your device.**

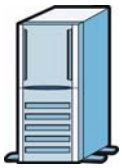
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

## Syntax Conventions

- The P-660H-Txv3s may be referred to as the "P-660H-T1v3s", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

## Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The P-660H-T1v3s icon is not an exact representation of your device.

| | | |
|---|---|---|
| P-660H-T1v3s | Computer | Notebook computer |
| Server  | Firewall | Telephone |
| Router | Switch | |

# Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

# Contents Overview

**User's Guide ..... 19**

Introduction ..... 21
The Web Configurator ..... 27
Status Screens ..... 33
Tutorials ..... 37
Setup Wizard ..... 57

**Technical Reference ..... 67**

WAN Setup ..... 69
LAN Setup ..... 89
Network Address Translation (NAT) ..... 105
Firewalls ..... 121
Filters ..... 125
Static Route ..... 131
802.1Q/1P ..... 135
Quality of Service (QoS) ..... 141
Dynamic DNS Setup ..... 149
Remote Management ..... 151
Universal Plug-and-Play (UPnP) ..... 161
System Settings ..... 171
Logs ..... 177
Tools ..... 179
Diagnostic ..... 193
Troubleshooting ..... 197
Product Specifications ..... 203

**Appendices and Index ..... 209**

# Table of Contents

**About This User's Guide ..... 3**

**Document Conventions ..... 5**

**Safety Warnings ..... 7**

**Contents Overview ..... 9**

**Table of Contents ..... 11**

**Part I: User's Guide ..... 19**

**Chapter 1**
**Introduction ..... 21**

1.1 Overview ..... 21
1.2 Ways to Manage the P-660H-T1v3s ..... 21
1.2.1 Good Habits for Device Management ..... 22
1.3 Applications ..... 22
1.3.1 Internet Access ..... 22
1.4 LEDs (Lights) ..... 23
1.5 The RESET Button ..... 24
1.5.1 Using the Reset Button ..... 25

**Chapter 2**
**The Web Configurator ..... 27**

2.1 Overview ..... 27
2.1.1 Accessing the Web Configurator ..... 27
2.2 Main Screen ..... 29
2.2.1 Title Bar ..... 30
2.2.2 Navigation Panel ..... 30
2.2.3 Main Window ..... 32
2.2.4 Status Bar ..... 32

**Chapter 3**
**Status Screens ..... 33**

3.1 Overview ..... 33
3.2 The Status Screen ..... 33

**Chapter 4**
**Tutorials ..... 37**

4.1 Overview ..... 37
4.2 Configuring the MAC Address Filter ..... 37
4.3 Setting Up NAT Port Forwarding ..... 38
4.3.1 Default Server ..... 39
4.3.2 Port Forwarding ..... 40
4.3.3 Special Note ..... 42
4.4 Access the P-660H-T1v3s Using DDNS ..... 43
4.4.1 Registering a DDNS Account on www.dyndns.org ..... 43
4.4.2 Configuring the P-660H-T1v3s for Remote Management ..... 44
4.4.3 Testing the DDNS Setting ..... 45
4.5 Configuring Static Route for Routing to Another Network ..... 46
4.6 Multiple Public and Private IP Address Mappings ..... 48
4.6.1 Full Feature NAT + Many-to-Many No Overload Mapping ..... 49
4.6.2 Full Feature NAT + One-to-One Mapping ..... 51
4.7 Multiple WAN Connections Example ..... 52
4.8 Multiple PVCs with QoS ..... 53
4.8.1 Configuring Multiple PVCs and ATM-QoS ..... 54

**Chapter 5**
**Setup Wizard ..... 57**

5.1 Overview ..... 57
5.2 Internet Access Wizard Setup ..... 57
5.2.1 Manual Configuration ..... 60

**Part II: Technical Reference ..... 67**

**Chapter 6**
**WAN Setup ..... 69**

6.1 Overview ..... 69
6.1.1 What You Can Do in the WAN Screens ..... 69
6.1.2 What You Need to Know ..... 69
6.1.3 Before You Begin ..... 70
6.2 The Internet Access Setup Screen ..... 71
6.2.1 Advanced Internet Access Setup ..... 75
6.3 The More Connections Screen ..... 77
6.3.1 More Connections Edit ..... 78
6.3.2 Configuring More Connections Advanced Setup ..... 81
6.4 WAN Technical Reference ..... 82
6.4.1 Encapsulation ..... 82

6.4.2 Multiplexing ..... 83
6.4.3 VPI and VCI ..... 84
6.4.4 IP Address Assignment ..... 84
6.4.5 Keep Alive/Nailed-Up Connection (PPP) ..... 84
6.4.6 NAT ..... 85
6.5 Traffic Shaping ..... 85
6.5.1 ATM Traffic Classes ..... 86

**Chapter 7**
**LAN Setup ..... 89**

7.1 Overview ..... 89
7.1.1 What You Can Do in the LAN Screens ..... 89
7.1.2 What You Need To Know ..... 89
7.1.3 Before You Begin ..... 91
7.2 The IP Screen ..... 91
7.2.1 The Advanced LAN IP Setup Screen ..... 92
7.3 The DHCP Setup Screen ..... 93
7.4 The Client List Screen ..... 94
7.5 The IP Alias Screen ..... 96
7.5.1 Configuring the LAN IP Alias Screen ..... 96
7.6 LAN Technical Reference ..... 98
7.6.1 LANs, WANs and the ZyXEL Device ..... 98
7.6.2 DHCP Setup ..... 98
7.6.3 DNS Server Addresses ..... 99
7.6.4 LAN TCP/IP ..... 99
7.6.5 RIP Setup ..... 101
7.6.6 Multicast ..... 101
7.6.7 Any IP ..... 102

**Chapter 8**
**Network Address Translation (NAT) ..... 105**

8.1 Overview ..... 105
8.1.1 What You Can Do in the NAT Screens ..... 105
8.1.2 What You Need To Know About NAT ..... 105
8.2 The NAT General Setup Screen ..... 107
8.3 The Port Forwarding Screen ..... 108
8.3.1 Configuring the Port Forwarding Screen ..... 109
8.3.2 The Port Forwarding Rule Edit Screen ..... 111
8.4 The Address Mapping Screen ..... 112
8.4.1 The Address Mapping Rule Edit Screen ..... 114
8.5 The SIP ALG Screen ..... 115
8.6 NAT Technical Reference ..... 116
8.6.1 NAT Definitions ..... 116

8.6.2 What NAT Does ....116
8.6.3 How NAT Works ....117
8.6.4 NAT Application ....118
8.6.5 NAT Mapping Types ....118
8.6.6 Port Translation ....119

**Chapter 9**
**Firewalls....121**

9.1 Overview .... 121
9.1.1 What You Can Do in the Firewall Screens .... 121
9.1.2 What You Need to Know .... 121
9.2 The Firewall Screen .... 123

**Chapter 10**
**Filters .... 125**

10.1 Overview .... 125
10.1.1 What You Can Do in the Filter Screens .... 125
10.1.2 What You Need to Know .... 125
10.2 The URL Filter Screen .... 126
10.3 The Application Filter Screen .... 127
10.4 The IP/MAC Filter Screen .... 128

**Chapter 11**
**Static Route .... 131**

11.1 Overview .... 131
11.1.1 What You Can Do in the Static Route Screens .... 131
11.2 The Static Route Screen .... 132
11.2.1 Static Route Edit .... 133

**Chapter 12**
**802.1Q/1P .... 135**

12.1 Overview .... 135
12.1.1 What You Can Do in the 802.1Q/1P Screens .... 135
12.1.2 What You Need to Know .... 135
12.2 The Group Setting Screen .... 137
12.2.1 Editing 802.1Q/1P Group Setting .... 138
12.3 The 802.1Q/1P Port Setting Screen .... 140

**Chapter 13**
**Quality of Service (QoS) .... 141**

13.1 Overview .... 141
13.1.1 What You Can Do in the QoS Screens .... 142
13.1.2 What You Need to Know .... 142

13.2 The QoS Screen ..... 143
13.2.1 The QoS Settings Summary Screen ..... 145
13.3 QoS Technical Reference ..... 146
13.3.1 IEEE 802.1p ..... 146
13.3.2 IP Precedence ..... 147
13.3.3 Automatic Priority Queue Assignment ..... 147

**Chapter 14**
**Dynamic DNS Setup ..... 149**

14.1 Overview ..... 149
14.1.1 What You Can Do in the DDNS Screen ..... 149
14.1.2 What You Need To Know About DDNS ..... 149
14.2 The Dynamic DNS Screen ..... 150

**Chapter 15**
**Remote Management ..... 151**

15.1 Overview ..... 151
15.1.1 What You Can Do in the Remote Management Screens ..... 152
15.1.2 What You Need to Know ..... 152
15.2 The WWW Screen ..... 153
15.2.1 Configuring the WWW Screen ..... 153
15.3 The Telnet Screen ..... 154
15.4 The FTP Screen ..... 155
15.5 The SNMP Screen ..... 156
15.6 The DNS Screen ..... 157
15.7 The ICMP Screen ..... 158

**Chapter 16**
**Universal Plug-and-Play (UPnP) ..... 161**

16.1 Overview ..... 161
16.1.1 What You Can Do in the UPnP Screen ..... 161
16.1.2 What You Need to Know ..... 161
16.2 The UPnP Screen ..... 163
16.2.1 Installing UPnP in Windows ..... 164
16.2.2 Using UPnP in Windows XP ..... 166

**Chapter 17**
**System Settings ..... 171**

17.1 Overview ..... 171
17.1.1 What You Can Do in the System Settings Screens ..... 171
17.1.2 What You Need to Know ..... 171
17.2 The General Screen ..... 172
17.3 The Time and Date Screen ..... 173

**Chapter 18**
**Logs ..... 177**

18.1 Overview ..... 177
18.1.1 What You Can Do in the Log Screens ..... 177
18.1.2 What You Need To Know ..... 177
18.2 The System Log Screen ..... 178

**Chapter 19**
**Tools ..... 179**

19.1 Overview ..... 179
19.1.1 What You Can Do in the Tool Screens ..... 179
19.1.2 What You Need To Know About Tools ..... 180
19.1.3 Before You Begin ..... 181
19.1.4 Tool Examples ..... 181
19.2 The Firmware Screen ..... 187
19.3 The Configuration Screen ..... 189
19.4 The Restart Screen ..... 192

**Chapter 20**
**Diagnostic ..... 193**

20.1 Overview ..... 193
20.1.1 What You Can Do in the Diagnostic Screens ..... 193
20.2 The General Diagnostic Screen ..... 193
20.3 The DSL Line Diagnostic Screen ..... 194

**Chapter 21**
**Troubleshooting ..... 197**

21.1 Power, Hardware Connections, and LEDs ..... 197
21.2 P-660H-T1v3s Access and Login ..... 198
21.3 Internet Access ..... 200

**Chapter 22**
**Product Specifications ..... 203**

22.1 Hardware Specifications ..... 203
22.2 Firmware Specifications ..... 204
22.3 Standards Support ..... 207

**Part III: Appendices and Index ..... 209**

Appendix A Setting up Your Computer's IP Address ..... 211

Appendix B Pop-up Windows, JavaScripts and Java Permissions ..... 235

Appendix C IP Addresses and Subnetting ..... 245

Appendix D Services ..... 255

Appendix E Legal Information ..... 259

**Index ..... 263**

# PART I
# User's Guide

# 1

# Introduction

## 1.1 Overview

The P-660H-T1v3s is an ADSL2+ router. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. The P-660HW-Tx v3 is also a complete security solution with a robust firewall and content filtering.

Please refer to the following description of the product name format.

- “H” denotes an integrated 4-port hub (switch).
- Models ending in “1”, for example P-660H-T1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in “3” denote a device that works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

**Only use firmware for your device’s specific model. Refer to the label on the bottom of your device.**

Note: All screens displayed in this user’s guide are from the P-660H-T1v3s model.

See the product specifications for a full list of features.

## 1.2 Ways to Manage the P-660H-T1v3s

Use any of the following methods to manage the P-660H-T1v3s.

- Web Configurator. This is recommended for everyday management of the P-660H-T1v3s using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.
- TR-069. This is an auto-configuration server used to remotely configure your device.

### 1.2.1 Good Habits for Device Management

Do the following things regularly to make the P-660H-T1v3s more secure and to manage the P-660H-T1v3s more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the P-660H-T1v3s to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the P-660H-T1v3s. You could simply restore your last configuration.

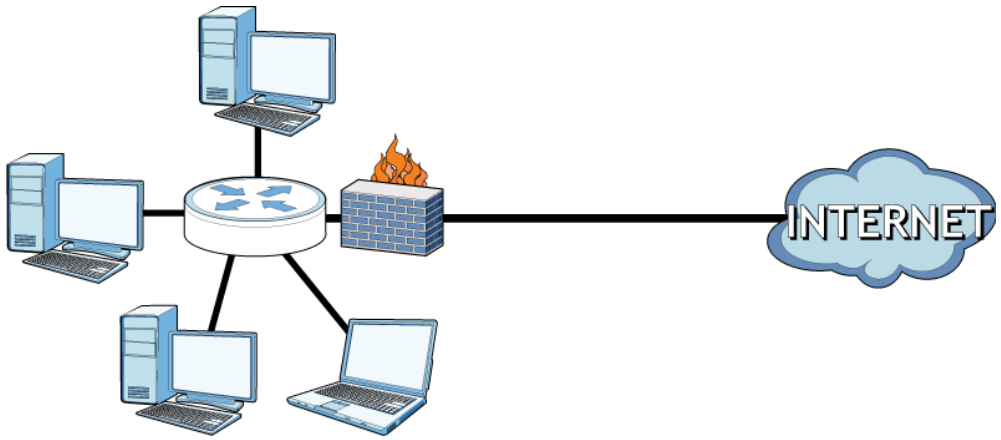
## 1.3 Applications

Here are some example uses for which the P-660H-T1v3s is well suited.

### 1.3.1 Internet Access

Your P-660H-T1v3s provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. Computers can connect to the P-660H-T1v3s's LAN ports.

**Figure 1** P-660H-T1v3s's Router Features




You can also configure firewall and content filtering on the P-660H-T1v3s for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

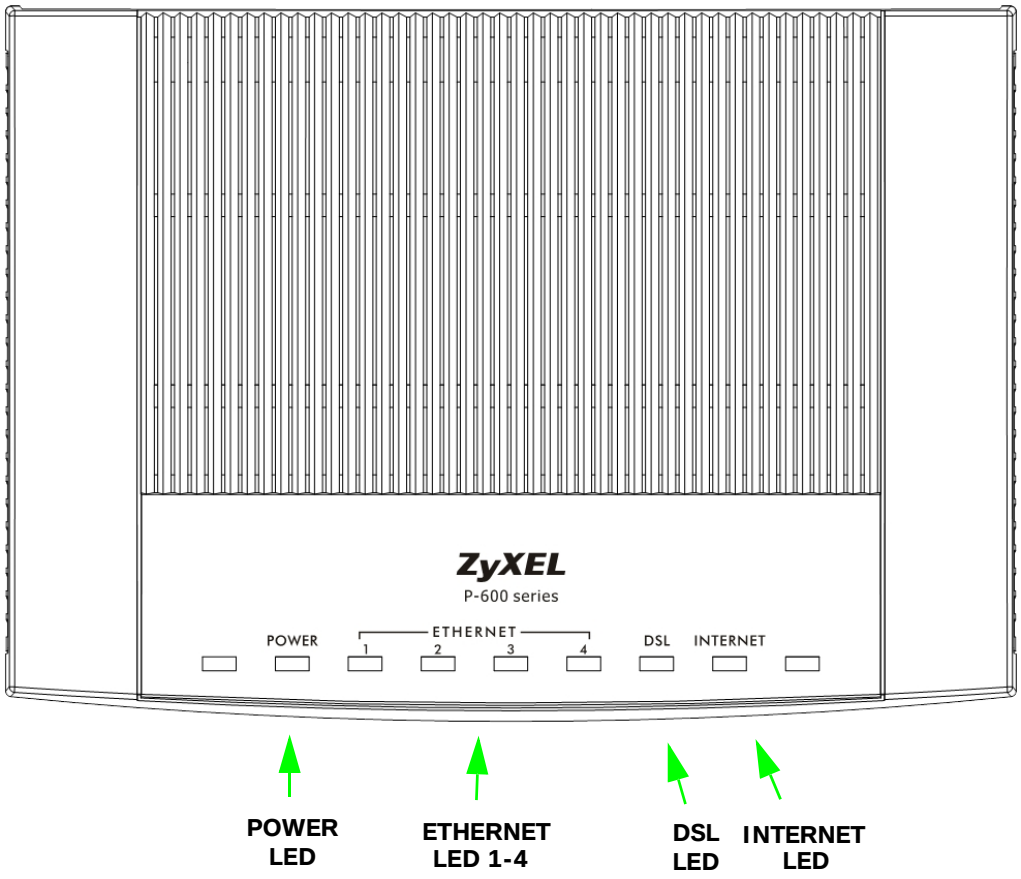
Use content filtering to block access to specific web sites, with URL's containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude particular computers on your network from content filtering. For example, you could block access to certain web sites for the kids.

Use QoS to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the P-660H-T1v3s gives voice over Internet calls high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

# 1.4 LEDs (Lights)

This section provides descriptions of the P-660H-T1v3s LEDs.

**Figure 2** Top Panel LEDs



The following table describes the labels in this picture.

**Table 1** LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| POWER | Green | On | The P-660H-T1v3s is receiving power and ready for use. |
| | Red | On | The P-660H-T1v3s detected an error while self-testing, or there is a device malfunction. |
| | | Off | The P-660H-T1v3s is not receiving power. |
| ETHERNET 1-4 | Green | On | The P-660H-T1v3s has an Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The P-660H-T1v3s is sending/receiving data, |
| | | Off | The P-660H-T1v3s does not have an Ethernet connection with the LAN. |
| DSL | Green | On | The DSL line is up. |
| | | Blinking | The P-660H-T1v3s is initializing the DSL line. |
| | | Off | The DSL line is down. |
| INTERNET | Green | On | The P-660H-T1v3s has an IP connection but no traffic.<br>Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up. |
| | | Blinking | The P-660H-T1v3s is sending or receiving IP traffic. |
| | Red | On | The P-660H-T1v3s attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed. |
| | | Off | The P-660H-T1v3s does not have an IP connection. |

Refer to the Quick Start Guide for information on hardware connections.

# 1.5 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”. You can also use the

### 1.5.1 Using the Reset Button

1. Make sure the **POWER** LED is on (not blinking).
2. To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

# 2

# The Web Configurator

## 2.1 Overview

The Web Configurator is an HTML-based management interface that allows easy device setup and management using a web browser.

The minimum requirements to use the Web Configurator:

- A modern web browser, such as Internet Explorer 7 or Firefox 3.5.
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

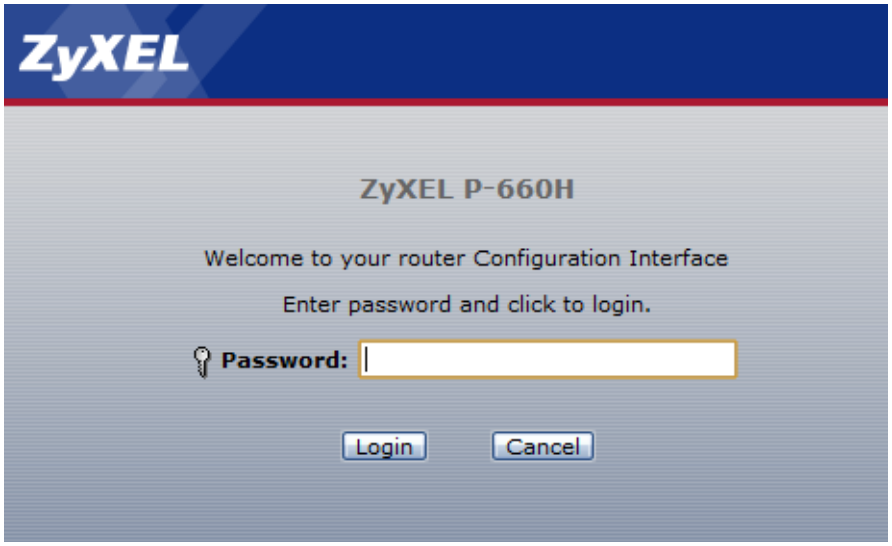
See Appendix B on page 235 if you need to make sure these functions are allowed in Internet Explorer.

### 2.1.1 Accessing the Web Configurator

1. Make sure your P-660H-T1v3s hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Enter "192.168.1.1" in the address bar.
4. A password screen displays. The P-660H-T1v3s has a dual login system. The default non-readable characters represents the user password (user by default). Clicking **Login without entering any password brings you to the system's status screen**. To access the administrative web configurator and manage the P-

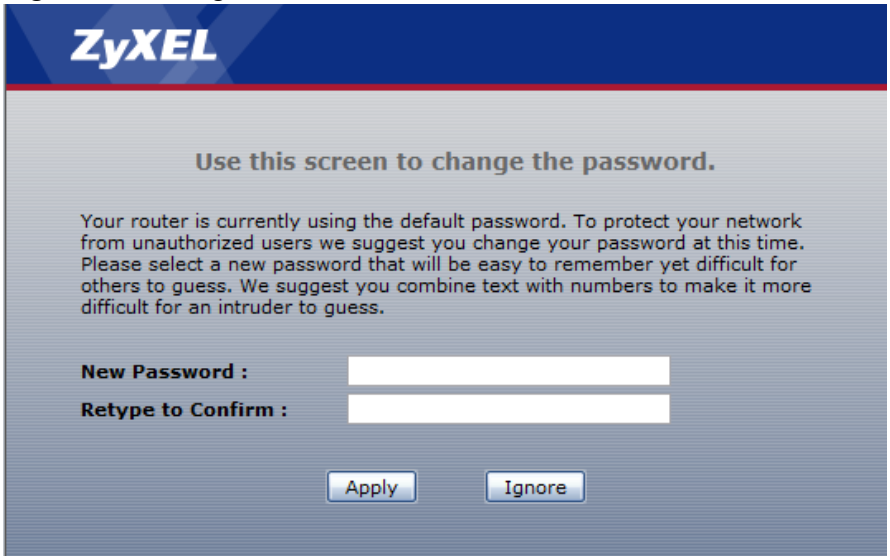
660H-T1v3s, type the admin password (1234 by default) in the password screen and click **Login**. Click **Cancel** to revert to the default user password in the password field. If you have changed the password, enter your password and click **Login**.

**Figure 3** Password Screen



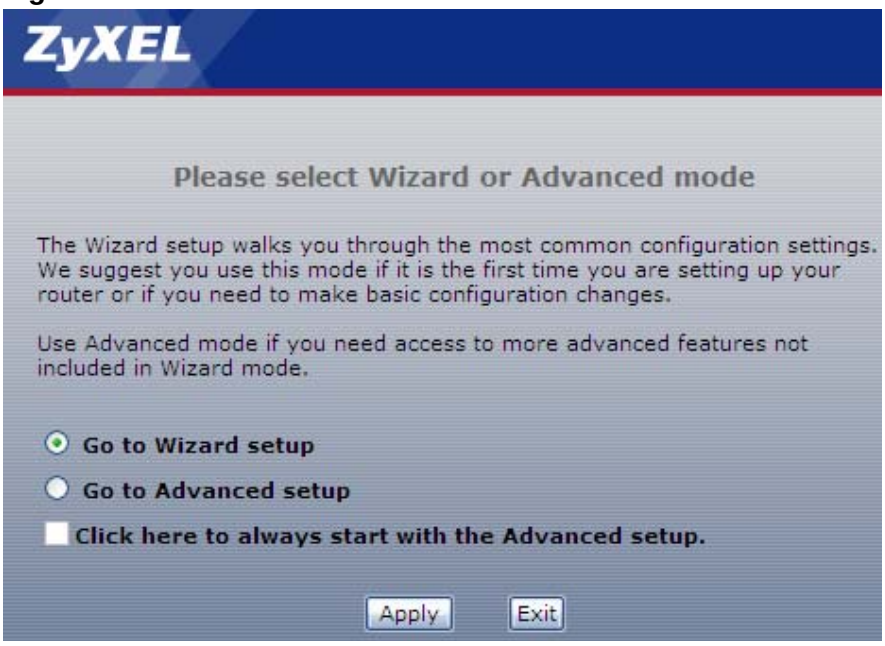

5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

**Figure 4** Change Password Screen


ZyXEL
Use this screen to change the password.
Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess. We suggest you combine text with numbers to make it more difficult for an intruder to guess.
New Password :
Retype to Confirm :
Apply
Ignore

6 Select **Go to Wizard setup** and click **Apply** to display the wizard main screen. Otherwise, select **Go to Advanced setup** and click **Apply** to display the **Status** screen.

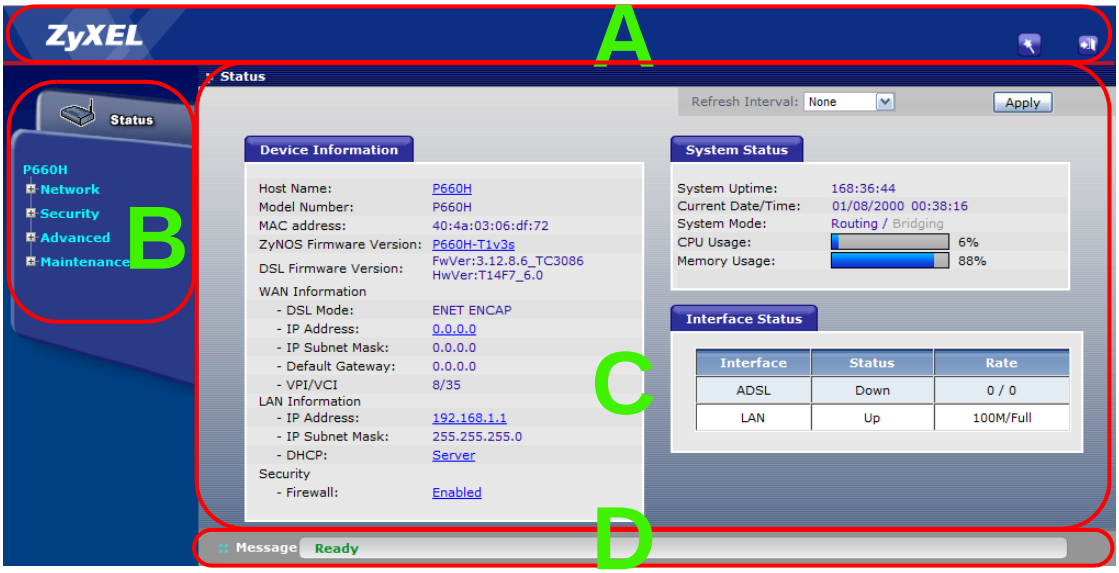
**Figure 5** Wizard or Advanced Mode Screen


ZyXEL
Please select Wizard or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.
Use Advanced mode if you need access to more advanced features not included in Wizard mode.
Go to Wizard setup
Go to Advanced setup
Click here to always start with the Advanced setup.
Apply
Exit

Note: For security reasons, the P-660H-T1v3s automatically logs you out if you do not use the Web Configurator for five minutes. If this happens, log in again.

# 2.2 Main Screen

**Figure 6** Main Screen



The main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

## 2.2.1 Title Bar

The title bar provides some icons in the upper right corner.

The icons provide the following functions.

**Table 2** Web Configurator Icons in the Title Bar

| ICON | DESCRIPTION |
|---|---|
| | **Wizard**<br>Click this icon to go to the configuration wizards. See Chapter 5 on page 57 for more information. |
| | **Logout**<br>Click this icon to log out of the web configurator. |

## 2.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure P-660H-T1v3s features. The following tables describe each menu item.

**Table 3** Navigation Panel Summary

| LINK | TAB | FUNCTION |
|---|---|---|
| Status | | This screen shows the P-660H-T1v3s's general device and network status information. Use this screen to access the statistics and client list. |
| Network | | |
| WAN | Internet Connection | Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties. |
| | More Connections | Use this screen to configure additional WAN connections. |

**Table 3** Navigation Panel Summary

| LINK | TAB | FUNCTION |
|---|---|---|
| LAN | IP | Use this screen to configure LAN TCP/IP settings, enable Any IP and other advanced properties. |
| | DHCP Setup | Use this screen to configure LAN DHCP settings. |
| | Client List | Use this screen to view current DHCP client information and to always assign specific IP addresses to individual MAC addresses (and host names). |
| | IP Alias | Use this screen to partition your LAN interface into subnets. |
| NAT | General | Use this screen to enable NAT. |
| | Port Forwarding | Use this screen to make your local servers visible to the outside world. |
| | ALG | Use this screen to enable or disable SIP ALG. |
| Security | | |
| Firewall | | Use this screen to activate/deactivate the firewall and the default action to take on network traffic going in specific directions. |
| Filter | URL | Use this screen to block access to specific web site URLs. |
| | Application Filter | Use this screen to block or allow specific Internet applications. |
| | IP/MAC Filter | Use this screen to configure the rules for IP filter sets. |
| Advanced | | |
| Static Route | | Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes. |
| 802.1Q/1P | Group Setting | Use this screen to activate 802.1Q/1P, specify the management VLAN group, display the VLAN groups and configure the settings for each VLAN group. |
| | Port Setting | Use this screen to configure the PVID and assign traffic priority for each port. |
| QoS | | Use this screen to enable QoS and traffic prioritizing, and configure bandwidth management on the WAN. |
| Dynamic DNS | | This screen allows you to use a static hostname alias for a dynamic IP address. |
| Remote MGMT | WWW | Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the P-660H-T1v3s. |
| | Telnet | Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the P-660H-T1v3s. |
| | FTP | Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the P-660H-T1v3s. |
| | SNMP | Use this screen to configure SNMP server port and access. |
| | DNS | Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the P-660H-T1v3s. |
| | ICMP | Use this screen to set whether or not your device will respond to pings and probes for services that you have not made available. |

**Table 3** Navigation Panel Summary

| LINK | TAB | FUNCTION |
|---|---|---|
| UPnP | | Use this screen to turn UPnP on or off. |
| Maintenance | | |
| System | General | Use this screen to configure your device's name, domain name, management inactivity timeout and password. |
| | Time and Date | Use this screen to change your P-660H-T1v3s's time and date. |
| Logs | | Use this screen to select which logs and/or immediate alerts your device is to record. |
| Tools | Firmware | Use this screen to upload firmware to your device. |
| | Configuration | Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings. |
| | Restart | This screen allows you to reboot the P-660H-T1v3s without turning the power off. |
| Diagnostic | General | Use this screen to test the connections to other devices. |
| | DSL Line | These screen displays information to help you identify problems with the DSL connection. |

## 2.2.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See Chapter 3 on page 33 for more information about the **Status** screen.

## 2.2.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

# 3

# Status Screens

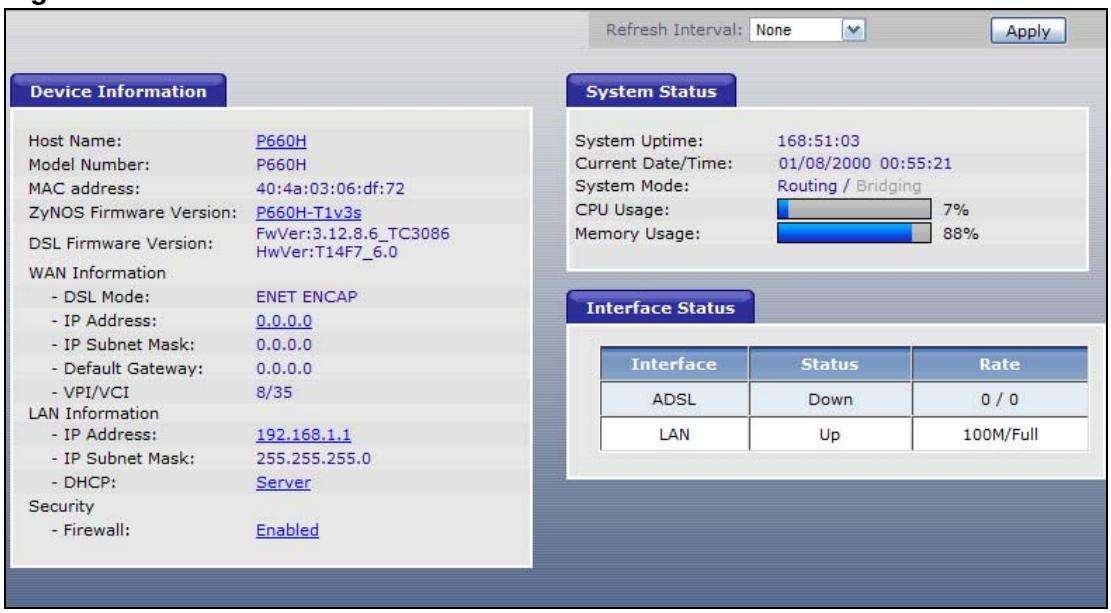
## 3.1 Overview

Use the **Status** screens to look at the current status of the device, system resources, and interfaces (LAN and WAN). The **Status** screen also provides detailed information from Any IP and DHCP and statistics from bandwidth management, and traffic.

## 3.2 The Status Screen

Use this screen to view the status of the P-660H-T1v3s. Click **Status** to open this screen.

**Figure 7** Status Screen



Each field is described in the following table.

**Table 4** Status Screen

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the P-660H-T1v3s to update this screen. |
| Apply | Click this to update this screen immediately. |
| Device Information | |
| Host Name | This field displays the P-660H-T1v3s system name. It is used for identification. You can change this in the **Maintenance > System > General** screen's **System Name** field. |
| Model Number | This is the model name of your device. |
| MAC Address | This is the MAC (Media Access Control) or Ethernet address unique to your P-660H-T1v3s. |
| ZyNOS Firmware Version | This is the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it. |
| DSL Firmware Version | This is the current version of the device's DSL modem code. |
| WAN Information | |
| DSL Mode | This is the DSL standard that your P-660H-T1v3s is using. |
| IP Address | This is the current IP address of the P-660H-T1v3s in the WAN. Click this to go to the screen where you can change it. |
| IP Subnet Mask | This is the current subnet mask in the WAN. |
| Default Gateway | This is the IP address of the default gateway, if applicable. |
| VPI/VCI | This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the wizard or **WAN** screen. |
| LAN Information | |
| IP Address | This is the current IP address of the P-660H-T1v3s in the LAN. Click this to go to the screen where you can change it. |
| IP Subnet Mask | This is the current subnet mask in the LAN. |
| DHCP | This field displays what DHCP services the P-660H-T1v3s is providing to the LAN. Choices are:<br><br>**Server** - The P-660H-T1v3s is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.<br><br>**Relay** - The P-660H-T1v3s acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.<br><br>**None** - The P-660H-T1v3s is not providing any DHCP services to the LAN.<br><br>Click this to go to the screen where you can change it. |

**Table 4** Status Screen

| LABEL | DESCRIPTION |
|---|---|
| Security | |
| Firewall | This displays whether or not the P-660H-T1v3s's firewall is activated. Click this to go to the screen where you can change it. |
| System Status | |
| System Uptime | This field displays how long the P-660H-T1v3s has been running since it last started up. The P-660H-T1v3s starts up when you plug it in, when you restart it (**Maintenance > Tools > Restart**), or when you reset it. |
| Current Date/Time | This field displays the current date and time in the P-660H-T1v3s. You can change this in **Maintenance > System > Time Setting**. |
| System Mode | This displays whether the P-660H-T1v3s is functioning as a router or a bridge. |
| CPU Usage | This field displays what percentage of the P-660H-T1v3s's processing ability is currently used. When this percentage is close to 100%, the P-660H-T1v3s is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 13 on page 141). |
| Memory Usage | This field displays what percentage of the P-660H-T1v3s's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the P-660H-T1v3s is probably becoming unstable, and you should restart the device. See Section 19.4 on page 192, or turn off the device (unplug the power) for a few seconds. |
| Interface Status | |
| Interface | This column displays each interface the P-660H-T1v3s has. |
| Status | This field indicates whether or not the P-660H-T1v3s is using the interface.<br><br>For the DSL interface, this field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation.<br><br>For the LAN interface, this field displays **Up** when the P-660H-T1v3s is using the interface and **Down** when the P-660H-T1v3s is not using the interface.<br><br>For the WLAN interface, it displays **Active** when WLAN is enabled or **InActive** when WLAN is disabled. |
| Rate | For the LAN interface, this displays the port speed and duplex setting.<br><br>For the DSL interface, it displays the downstream and upstream transmission rate.<br><br>For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or **N/A** when WLAN is disabled. |

# 4

# Tutorials

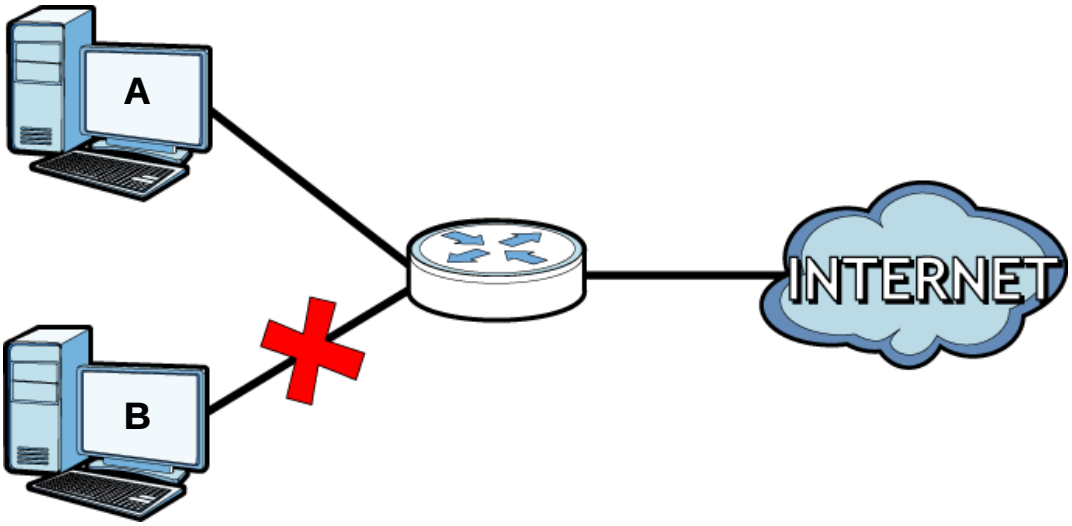
## 4.1 Overview

This chapter shows you how to use the P-660H-T1v3s's various features.

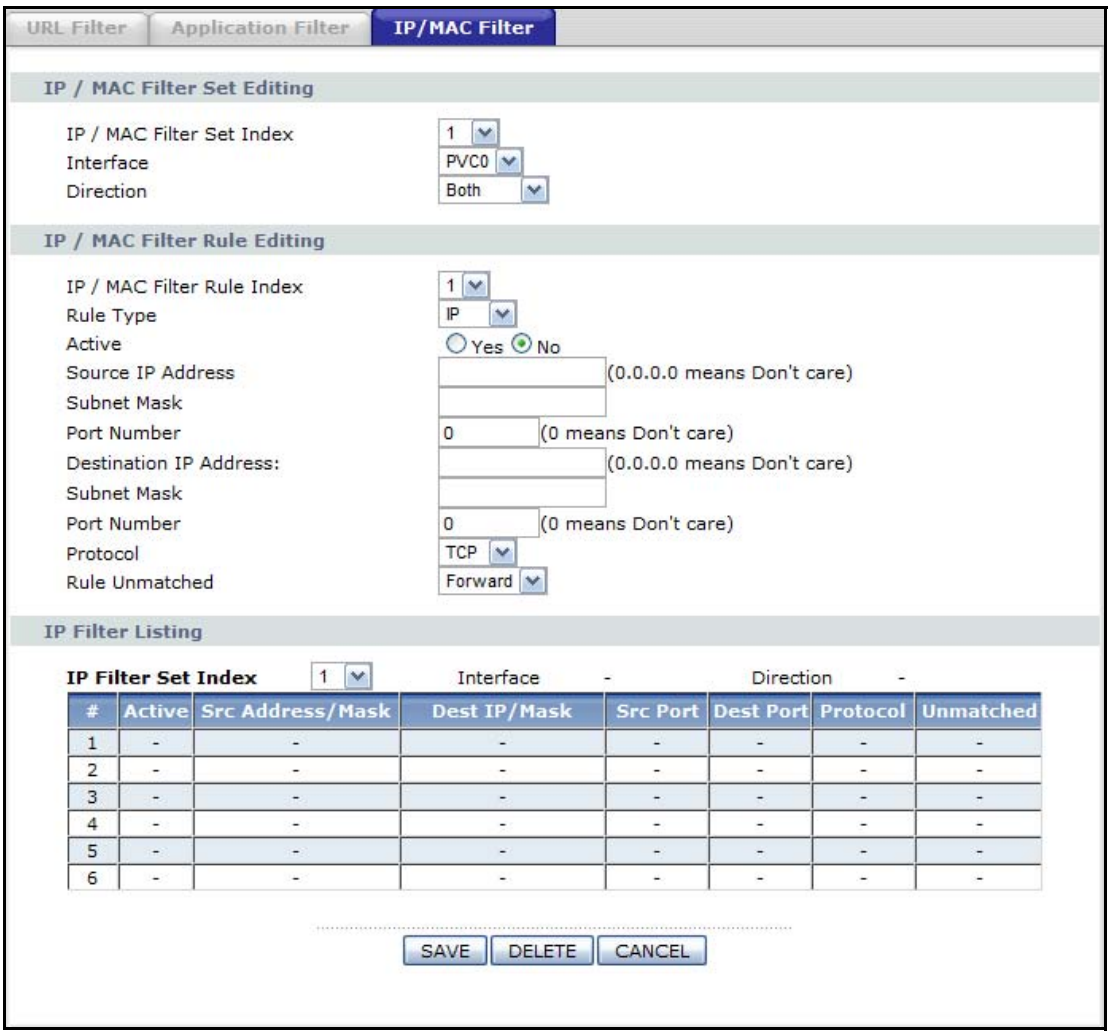
- Configuring the MAC Address Filter
- Setting Up NAT Port Forwarding
- Access the P-660H-T1v3s Using DDNS
- Configuring Static Route for Routing to Another Network
- Multiple Public and Private IP Address Mappings
- Multiple WAN Connections Example
- Multiple PVCs with QoS

## 4.2 Configuring the MAC Address Filter

This tutorial shows you how to configure MAC address filter to prevent certain computers from accessing the Internet. In this example, computer **A** will have unlimited Internet access, while computer **B** will not.



1 Click **Security** > **Filter** > **IP/MAC Filter** to open the following screen.




2 For **Rule Type**, select **MAC**.

3 Enter the **MAC Address** of the computer (**B**) that you want to block.

4 Click the **SAVE** button.

# 4.3 Setting Up NAT Port Forwarding

This tutorial shows you how to configure the port settings on a P-660H-T1v3s to allow an Xbox to communicate with the online Xbox live service.

Xbox 360 requires the following ports to be available in order to connect to the Xbox LIVE service:

TCP: 53, 80, 3074

UDP: 53, 88, 3074

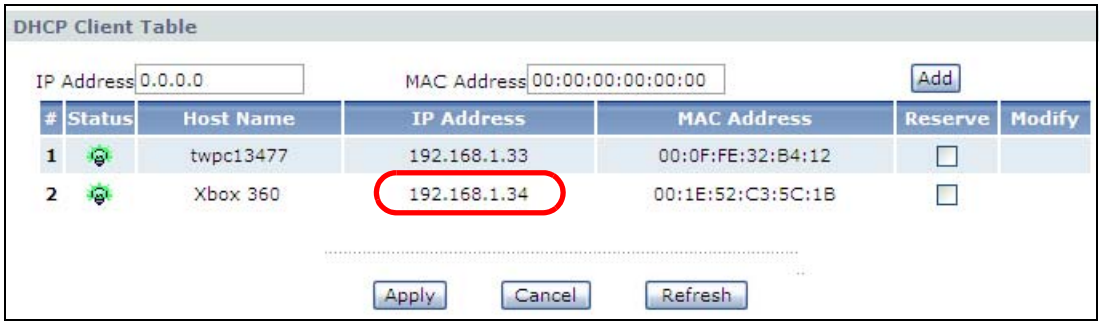
You can set up the port settings in two waysL: either set the Xbox 360's IP address as the default server; or configure the port settings for Xbox 360.

## 4.3.1 Default Server

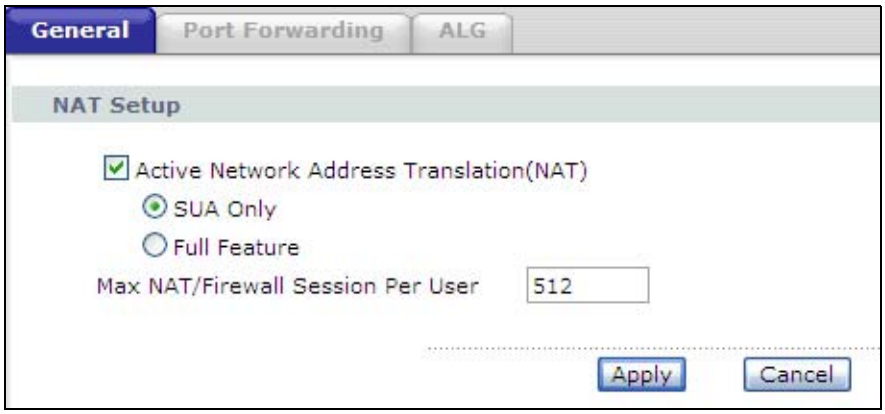
It is much easier to set the Xbox 360's IP address as the default server if it is not already assigned to another server. There is no need to enter any port number.

Note: Setting a device as the default server exposes the device to potential attacks. Any port service trying to access the P-660H-T1v3s's WAN IP address will be forwarded to the default server. It is recommended that you set up a firewall rule to protect the device.

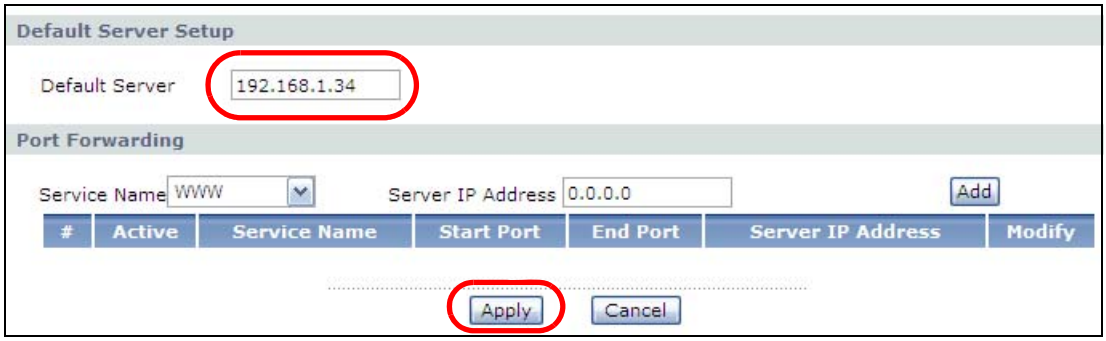
1 If you are not certain about the Xbox 360's IP address, you may check it in the DHCP client table. Click **Network** > **LAN** > **Client List** to open the following screen. Look for the IP address for Xbox 360.




2 Click **Network** > **NAT** to open the **General** screen. Select **Active Network Address Translation** and **SUA Only**. Click **Apply**.



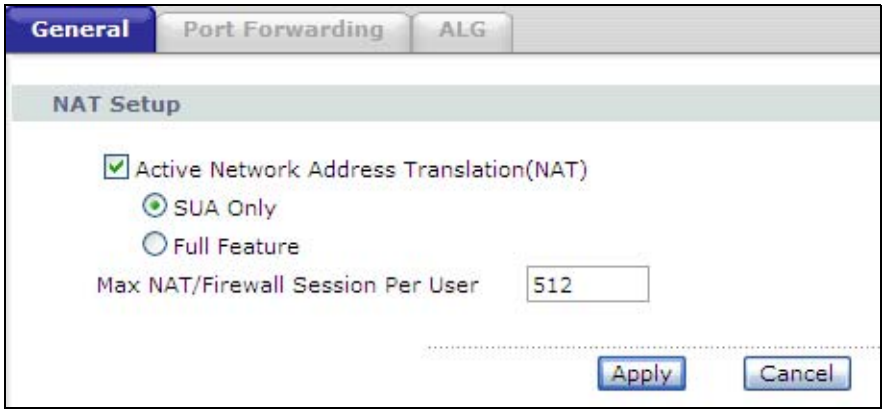
3 Click **Network** > **NAT > Port Forwarding**. Enter the Xbox 360's IP address in the **Default Server** field. Click **Apply**.



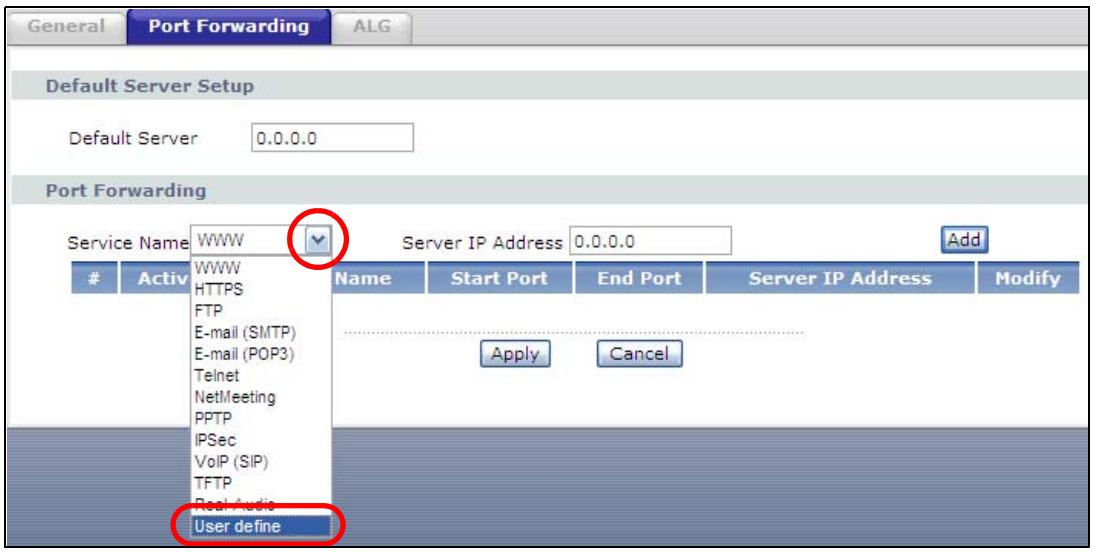

## 4.3.2 Port Forwarding

If the default server is already assigned to another server, configure the ports for Xbox 360.

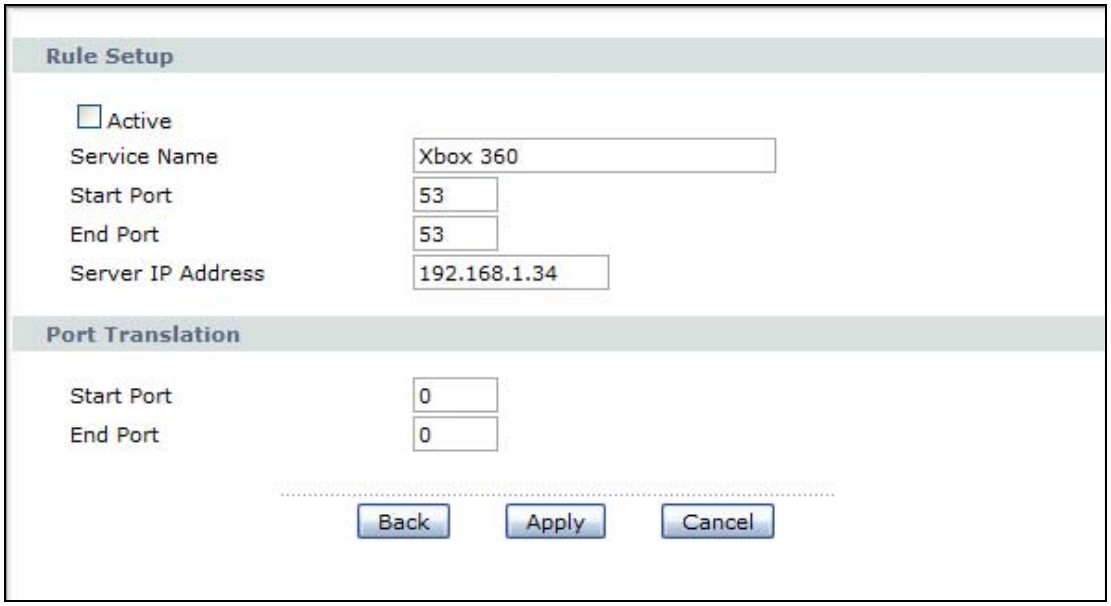
1 Click **Network** > **NAT** to open the **General** screen. Select **Active Network Address Translation** and **SUA Only**. Click **Apply**.



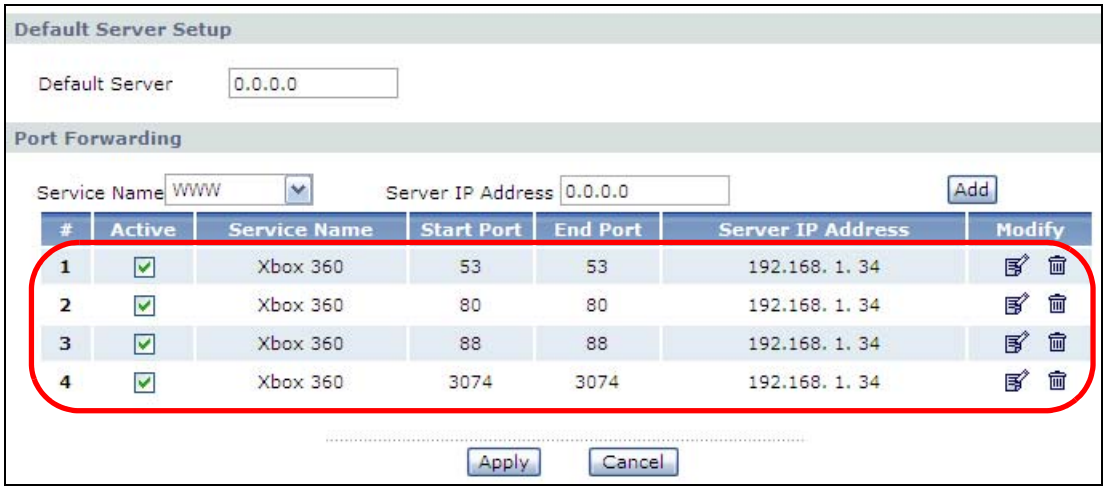
2 Click **Network** > **NAT** > **Port Forwarding**. Select **User define** from the **Service Name** field.




3 Configure the screen as follows to open TCP/UDP port 53 for Xbox 360. Click **Apply**.



4 Repeat steps 2 and 3 to open the rest of the ports for Xbox 360. The port forwarding settings you configured are listed in the **Port Forwarding** screen.


Default Server Setup
Default Server 0.0.0.0
Port Forwarding
Service Name WWW
Server IP Address 0.0.0.0
Add
# Active Service Name Start Port End Port Server IP Address Modify
1 Xbox 360 53 53 192.168. 1. 34
2 Xbox 360 80 80 192.168. 1. 34
3 Xbox 360 88 88 192.168. 1. 34
4 Xbox 360 3074 3074 192.168. 1. 34
Apply
Cancel

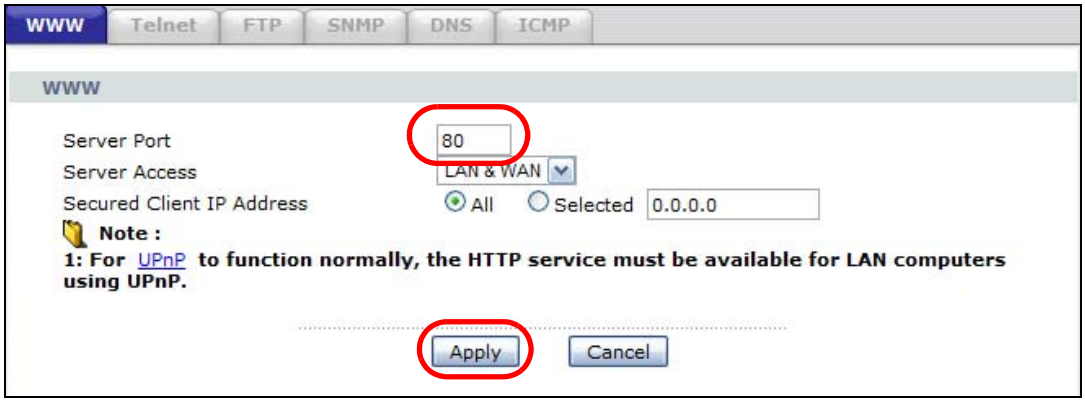
## 4.3.3 Special Note

In this tutorial, all port 80 traffic is forwarded to Xbox 360, but port 80 is also the default listening port for remote management via WWW. If you also want to manage the P-660H-T1v3s from the Internet, you need to assign an unused port for WWW remote access.

1 Click **Advanced** > **Remote MGMT** to open the **WWW** screen.

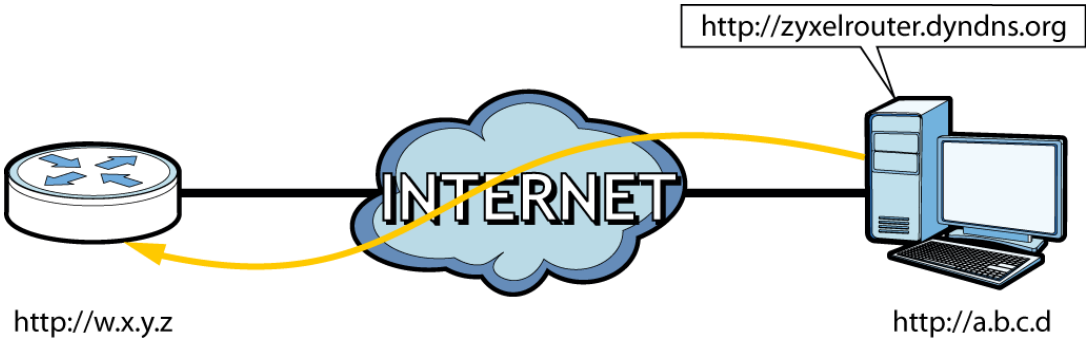
2 Enter an unused port in the **Port** field (this example uses 81).

3 Click **Apply**.



# 4.4 Access the P-660H-T1v3s Using DDNS

If you connect your P-660H-T1v3s to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The P-660H-T1v3s's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the P-660H-T1v3s using a domain name.




To use this feature, you have to apply for DDNS service at www.dyndns.org.

Note: If you have a private WAN IP address, then you cannot use DDNS.

## 4.4.1 Registering a DDNS Account on www.dyndns.org

1. Open a browser and type **http://www.dyndns.org**.
2. Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
3. Log into www.dyndns.org using your account.
4. Add a new DDNS host name. This tutorial uses the following settings as an example.
   - Hostname: **zyxelrouter.dyndns.org**
   - Service Type: **Host with IP address**
   - IP Address: Enter the WAN IP address that your P-660H-T1v3s is currently using. You can find the IP address on the Web Configurator **Status** page.

   Then you will need to configure the same account and host name on the P-660H-T1v3s later.

## 4.4.2 Configuring the P-660H-T1v3s for Remote Management

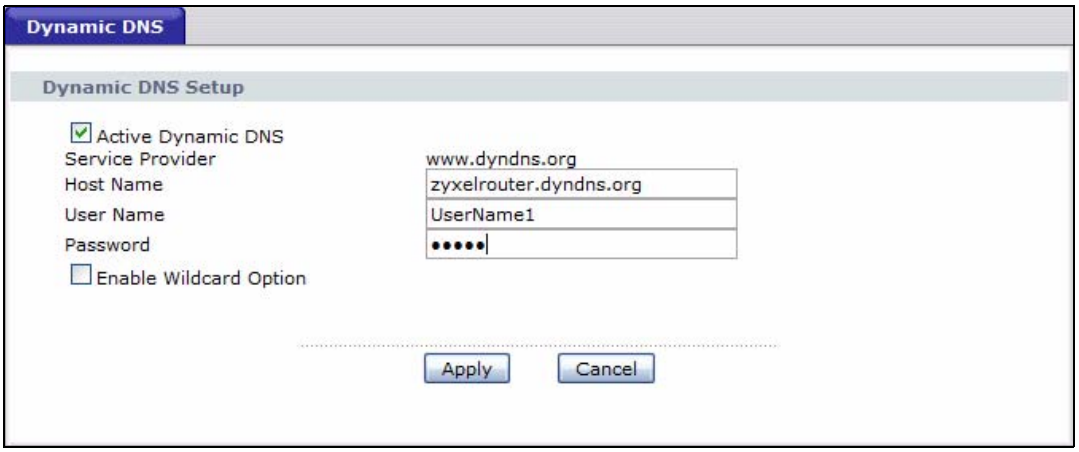
By default, your P-660H-T1v3s firewall is enabled to secure your network from external access. In this section, you activate DDNS with the settings from the previous section, and then modify the Remote Management settings to allow a connection to be initiated from a single external IP address.

**1** Configure the following settings in the **Advanced** > **Dynamic DNS** screen.

**1a** Select **Active Dynamic DNS**.

**1b** In the **Host Name** field, enter 'zyxelrouter.dyndns.org'.

**1c** Enter the **User Name** ('UserName1') and **Password** ('12345').




**2** Click **Apply**.

**3** Click **Advanced > Remote MGMT > WWW**.

4 The **WWW** screen opens.

Configure the following settings:

**Server Port**: The default web (HTTP) port that allows traffic to and from the WAN is 80. If you open this port to allow for external communication requests, then that would make quite a hole in the device's security. So enter '81' instead.

**Server Access**: Set this to WAN, to limit management requests to WAN only. This prevents attempts from the LAN-side of the P-660H-T1v3s.

**Secured Client IP Address**: Choose Selected, then enter the WAN IP address from which you intend to connect to the P-660H-T1v3s. This means only connections from that IP address are allowed to open the port.

5 Click **Apply**.

## 4.4.3 Testing the DDNS Setting

Now you should be able to access the P-660H-T1v3s from the Internet. To test this:

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

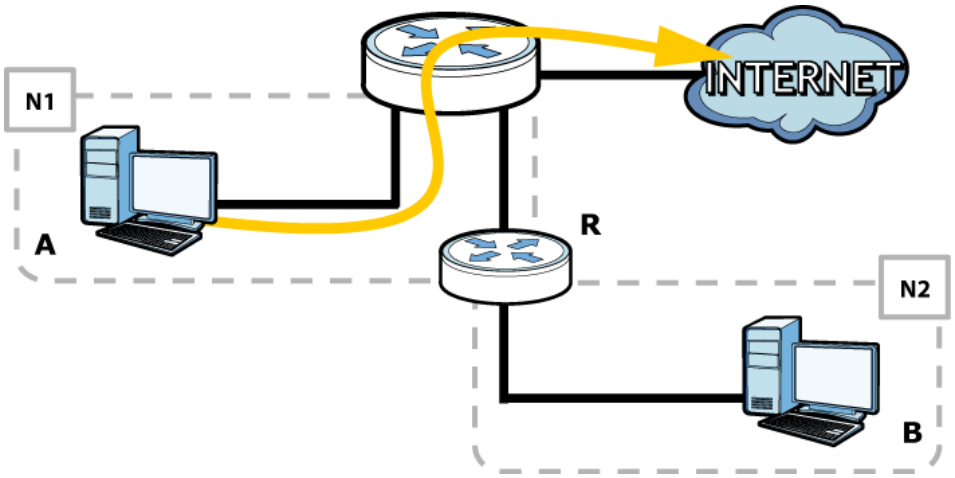
2 Type **http://zyxelrouter.dyndns.org** and press [Enter].

3 The P-660H-T1v3s's login page should appear. You can then log into the P-660H-T1v3s and manage it.

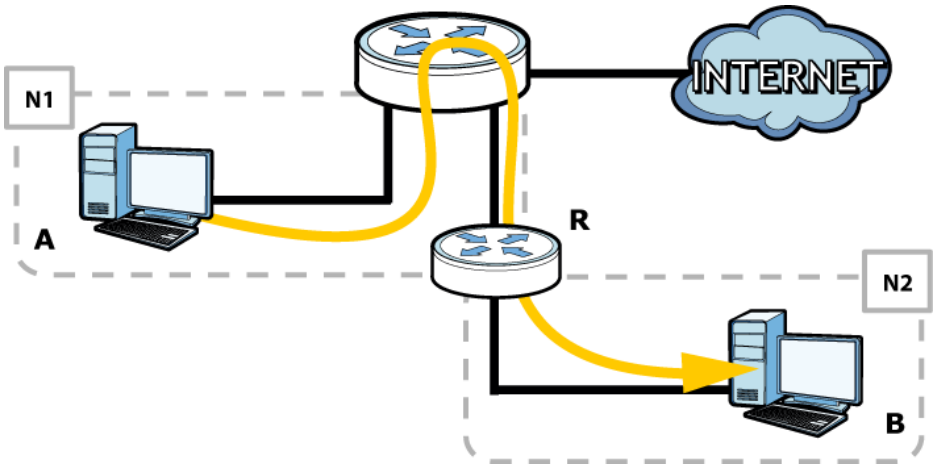
# 4.5 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the P-660H-T1v3s's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the P-660H-T1v3s's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the P-660H-T1v3s's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the P-660H-T1v3s to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the P-660H-T1v3s routes traffic from **A** to **R** and then **R** routes the traffic to **B**.




This tutorial uses the following example IP settings:

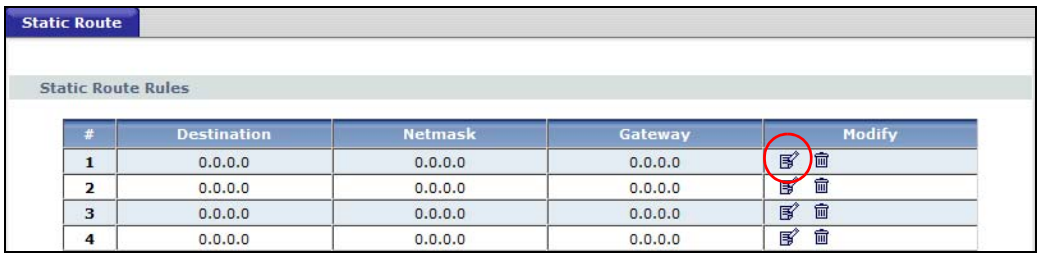
**Table 5** IP Settings in this Tutorial

| DEVICE / COMPUTER | IP ADDRESS |
|---|---|
| The P-660H-T1v3s's WAN | 172.16.1.1 |
| The P-660H-T1v3s's LAN | 192.168.1.1 |
| **A** | 192.168.1.34 |
| **R**'s N1 | 192.168.1.253 |
| **R**'s N2 | 192.168.10.2 |
| **B** | 192.168.10.33 |

To configure a static route to route traffic from **N1** to **N2**:

1 In the Web Configurator, click **Advanced** > **Static Route**.

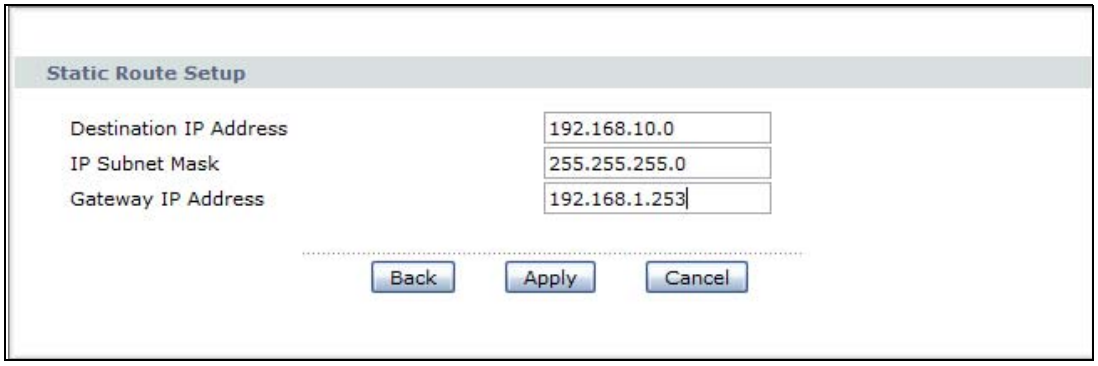
2 Click **Edit** on a new rule in the **Static Route** screen.



3 Configure the **Static Route Setup** screen using the following settings:

**3a** Enter a destination IP address of **192.168.10.0** and a subnet mask **255.255.255.0** for N2.

**3b** Enter **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.

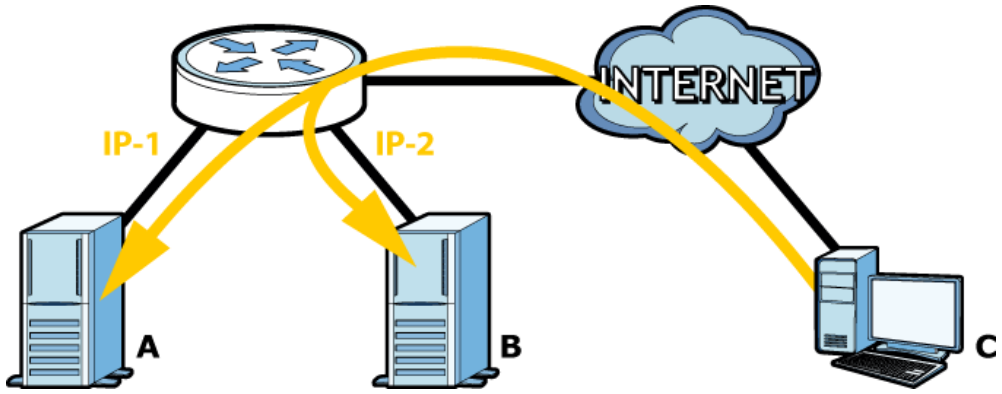



**3a** Click **Apply**.

Now **B** should be able to receive traffic from **A**.

# 4.6 Multiple Public and Private IP Address Mappings

If your ISP gives you more than one static IP address for your Internet access, you can map each IP address for a specific service. This tutorial assumes you are given two static public IP addresses which you want to map to the pair of servers labeled **A** and **B**.



This tutorial uses the following example settings:

**Table 6** IP Settings in this Tutorial

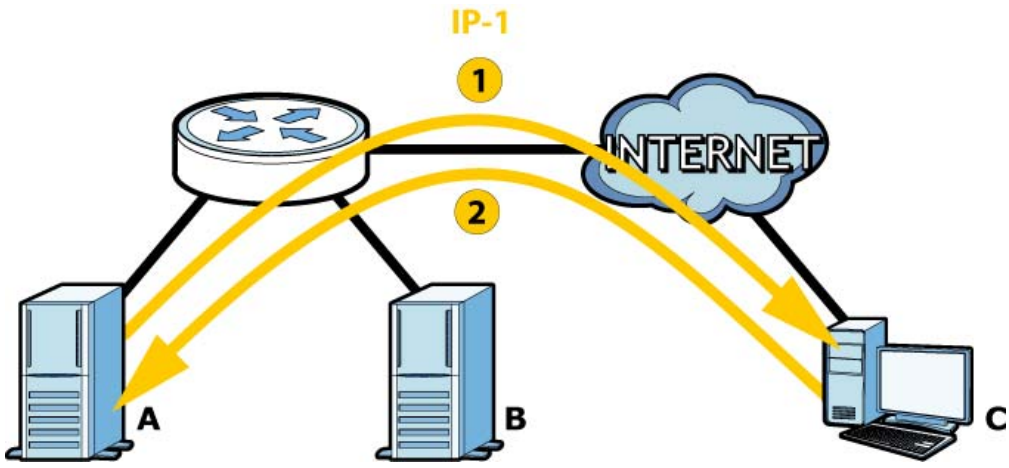
| DEVICE / COMPUTER | IP ADDRESS |
|---|---|
| The P-660H-T1v3s's WAN | 172.16.1.253 (**IP-1**)<br>172.16.1.254 (**IP-2**) |
| The P-660H-T1v3s's LAN | 192.168.1.1 |
| **A** | 192.168.1.2 |
| **B** | 192.168.1.3 |
| C | a.b.c.d |

To do this, you can use either of the following settings:

- Full Feature NAT with many-to-many no overload mapping
- Full Feature NAT with one-to-one mapping

## 4.6.1 Full Feature NAT + Many-to-Many No Overload Mapping

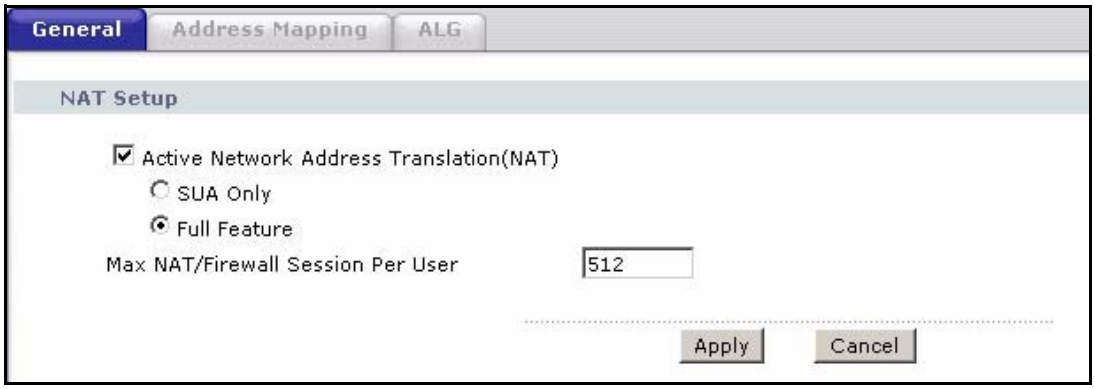
Use this setting if your applications can use random public IP addresses and the applications are initiated from the Intranet computers (**A** and **B**). For example, VoIP application. See Section 4.6.2 on page 51 if it is not.




To configure this:

1 Click **Network** > **NAT**.

2 Select **Active Network Address Translation(NAT)** and **Full Feature** in the **General** screen. Click **Apply**.




3 Click the **Address Mapping** tab, and then click the **Edit** icon on a new rule.

General
Address Mapping
ALG
Address Mapping Rules
# Local Start IP Local End IP Global Start IP Global End IP Type Modify
1 - - - - -
2 - - - - -

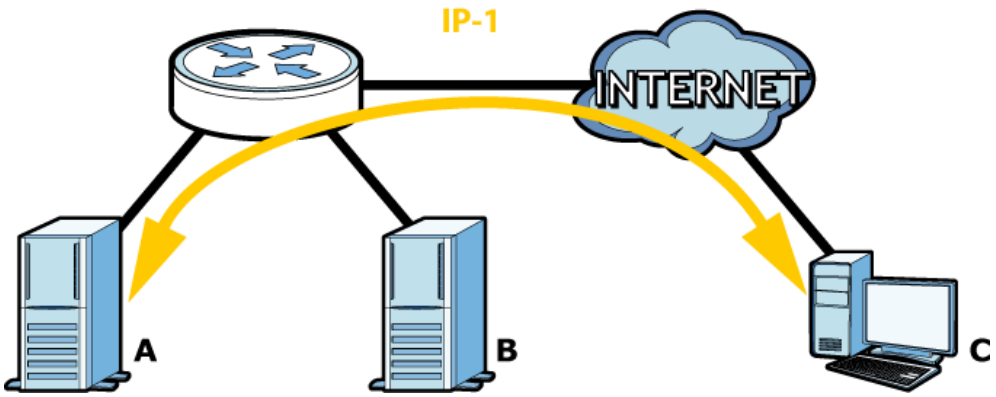
4 Configure the rule using the following settings:

- Type: **Many-to-Many No Overload**
- Local IP addresses: **192.168.1.2** ~ **192.168.1.3**
- Global IP addresses: **172.16.1.253** ~ **172.16.1.254**

5 Click **Apply**.

## 4.6.2 Full Feature NAT + One-to-One Mapping

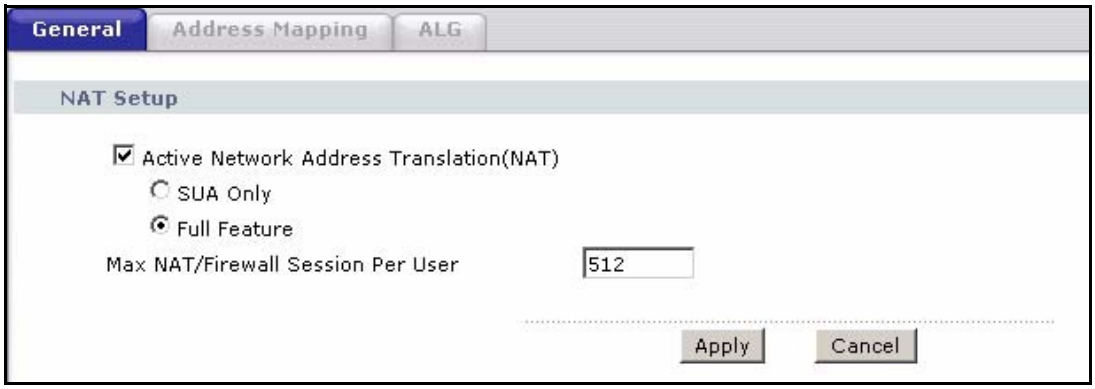
Use this setting if your applications must use fixed public IP addresses and the applications can be initiated either from the Intranet computers (**A** and **B**) or the Internet computer (**C**). For example, gaming application.




To configure this setting:

1 Click **Network** > **NAT**.

2 Select **Active Network Address Translation(NAT)** and **Full Feature** in the **General** screen. Click **Apply**.




3 Click the **Address Mapping** tab, click the **Edit** icon on a new rule.

4 Configure two rules for the one-to-one mappings:

- Rule 1 (This maps the public IP address 172.16.1.253 to the private IP address 192.168.1.2)

  Type: **One-to-One**

  Local Start IP: **192.168.1.2**

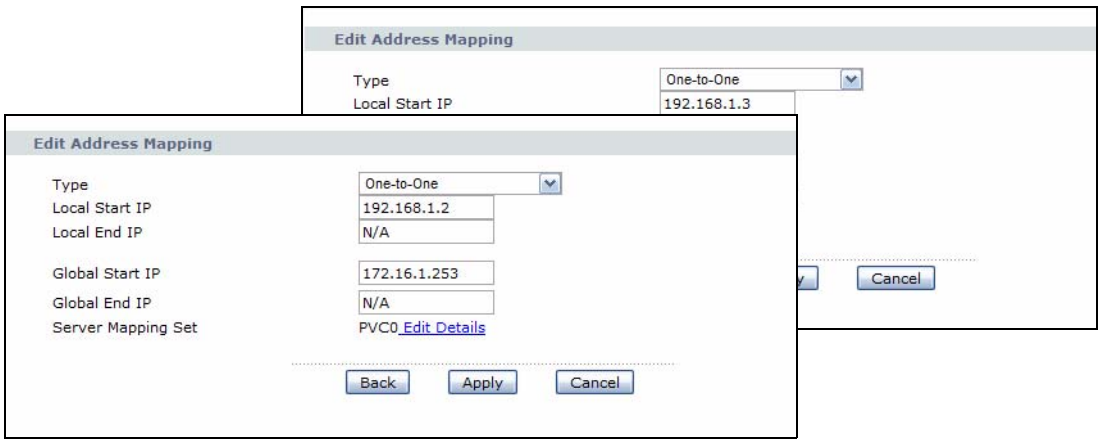
  Global Start IP: **172.16.1.253**

- Rule 2 (This maps the public IP address 172.16.1.254 to the private IP address 192.168.1.3)

  Type: **One-to-One**

  Local Start IP: **192.168.1.3**

  Global Start IP: **172.16.1.254**




Click **Apply** on each of the screens.

# 4.7 Multiple WAN Connections Example

This example shows an application for multiple WAN connections.

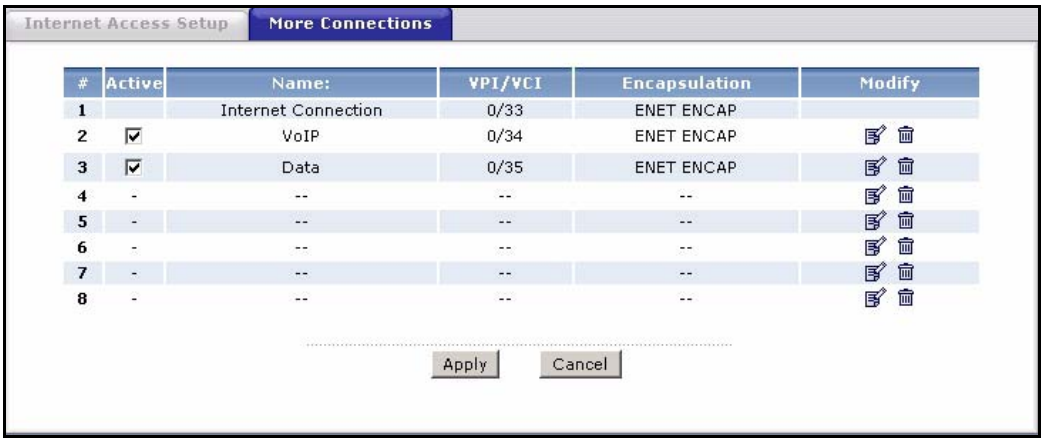
Your ISP may configure more than one WAN connection on the P-660H-T1v3s to record traffic statistics or calculate service charges.

In Figure 8, three WAN connections are configured over the ADSL line:

- The connection with VPI/VCI, **0/33**, is dedicated for Media-On-Demand (MOD) service.
- The connection with VPI/VCI, **0/34**, is dedicated for VoIP service.

- The connection with VPI/VCI, **0 / 35**, is dedicated for general data transmission.

**Figure 8** Example for Multiple WAN Connections

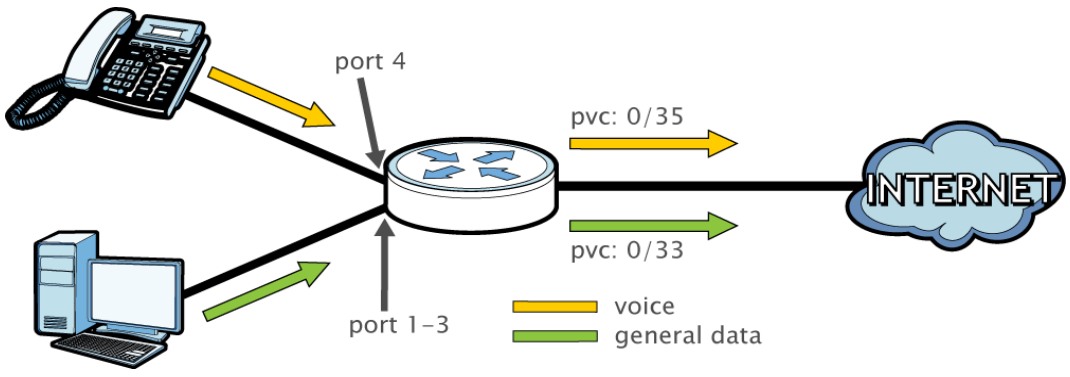

Internet Access Setup
More Connections
# Active Name: VPI/VCI Encapsulation Modify
1 Internet Connection 0/33 ENET ENCAP
2 VoIP 0/34 ENET ENCAP
3 Data 0/35 ENET ENCAP
4 - -- -- --
5 - -- -- --
6 - -- -- --
7 - -- -- --
8 - -- -- --
Apply
Cancel

# 4.8 Multiple PVCs with QoS

This tutorial is only applicable for an ISP engineer.

An ISP may configure multiple PVCs for seperating different subscriber application traffic. This helps to record traffic statistics or calculate service charges. In addition, the ISP can also apply different QoS according to the application importance and whether the application is time-sensitive or not.

In the following figure, the P-660H-T1v3s is configured to transmit two types of traffic, VoIP using SIP and general data using 0/33 and 0/35 PVCs respectively. Because voice traffic is considered to transmit continuously but not for general data, this tutorial uses Constant Bit Rate (CBR) for VoIP and Unspecified Bit Rate (UBR) for general data ATM-QoS setting.



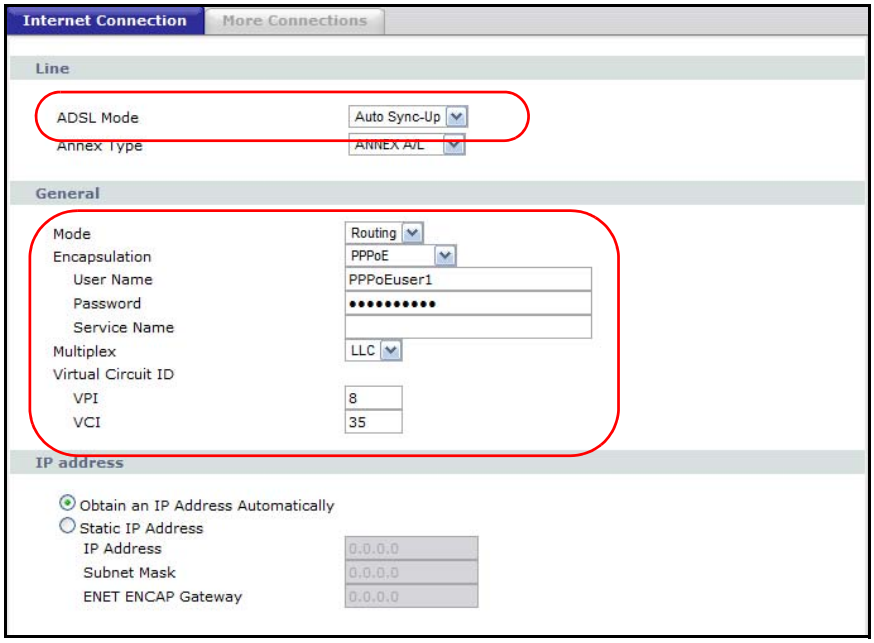

This tutorial also dedicates the P-660H-T1v3s LAN port 4 for voice and ports 1~3 for general data traffic.

## 4.8.1 Configuring Multiple PVCs and ATM-QoS

This section shows you how to configure two PVCs and specify a proper ATM-QoS type for each PVC.

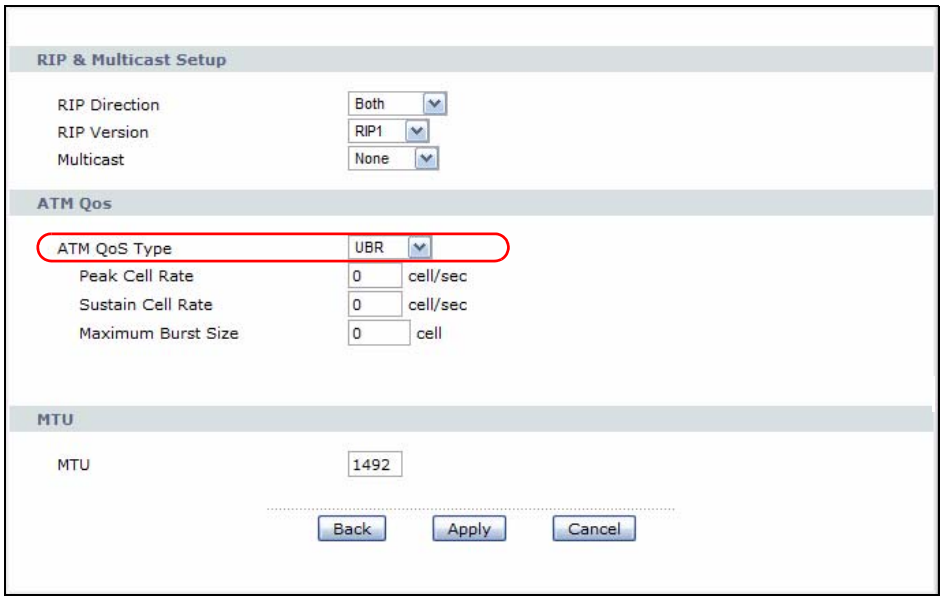
1 Click **Network** > **WAN** > **Internet Access Setup**, configure the settings you (ISP) want to provide to the subscriber for general data transmission. This tutorial uses the following example settings:

- ADSL Mode: **Auto Sync-Up**
- Mode: **Routing**
- Encapsulation: **PPPoE**
- User Name: **PPPoEuser1**
- Password: **1234**
- Multiplex: **LLC**
- VPI: **0**
- VPC: **35**



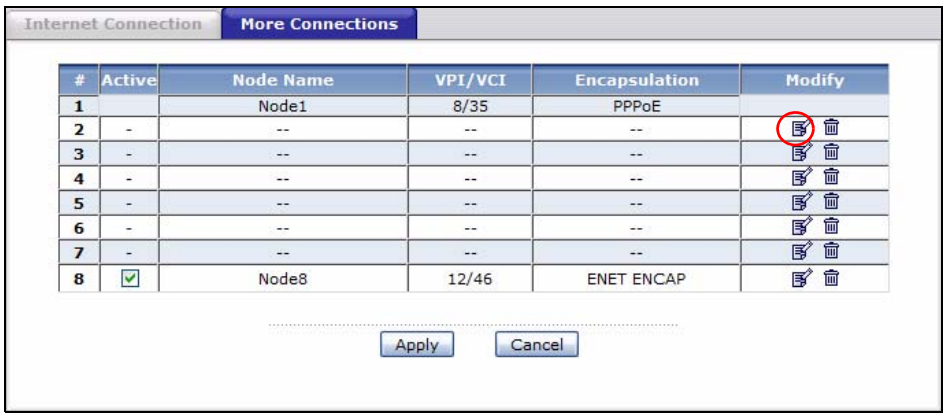

Leave the other settings as their defaults and click **Apply**.

2 Click the **Advanced Setup** button to display the following options. Select **UBR** in the **ATM QoS Type** field.



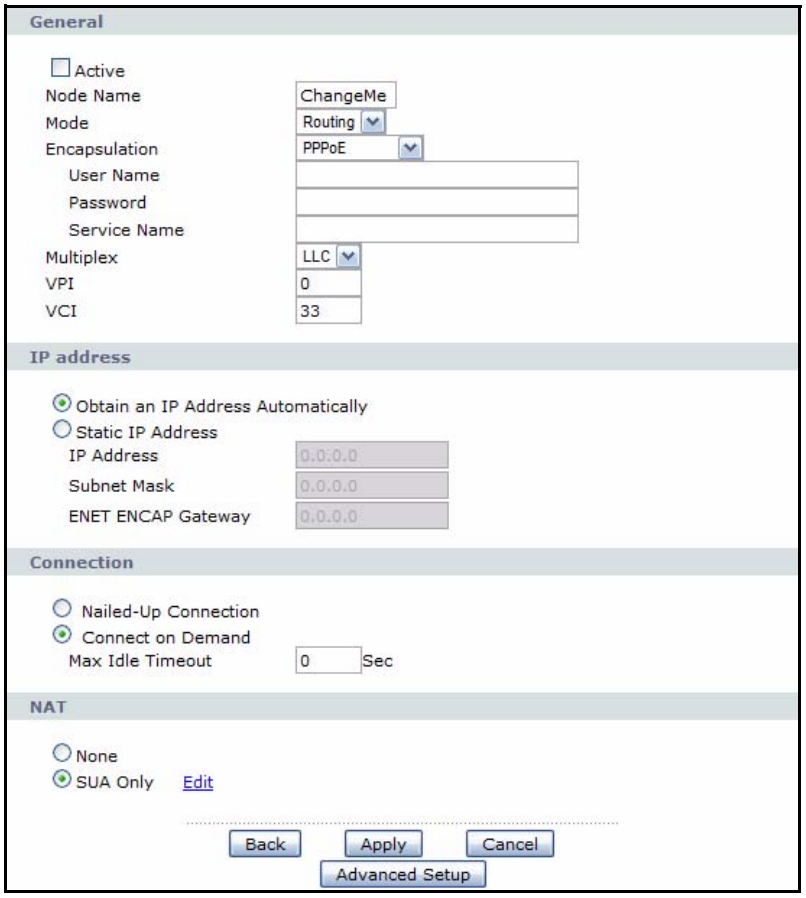

Click **Apply**.

3 Click the **More Connections** tab and then click the **Edit** icon next for an entry.


Internet Connection
More Connections
# Active Node Name VPI/VCI Encapsulation Modify
1 Node1 8/35 PPPoE
2 - -- -- --
3 - -- -- --
4 - -- -- --
5 - -- -- --
6 - -- -- --
7 - -- -- --
8 Node8 12/46 ENET ENCAP
Apply
Cancel

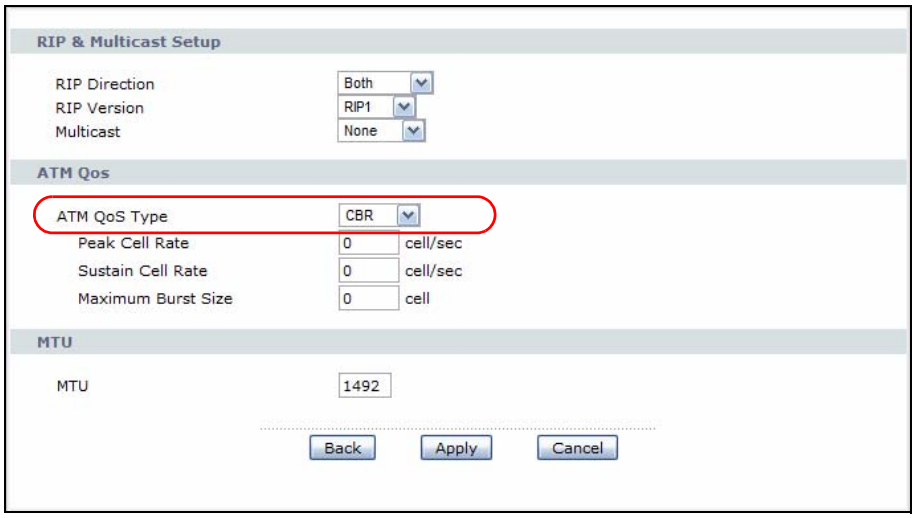
4 Then configure the screen using the following example settings:

- Select **Active**.
- Name: **PVCVoIP**
- Mode: **Routing**
- Encapsulation: **ENET ENCAP**
- Multiplex: **LLC**
- VPI: **0**
- VCI: **33**




Click **Apply**.

5 Click the **Advanced Setup** button and then select **CBR** in the **ATM QoS Type** field.




Click **Apply**.

# 5

# Setup Wizard

## 5.1 Overview

Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP.

Note: See the advanced menu chapters for detailed information on these fields.

## 5.2 Internet Access Wizard Setup

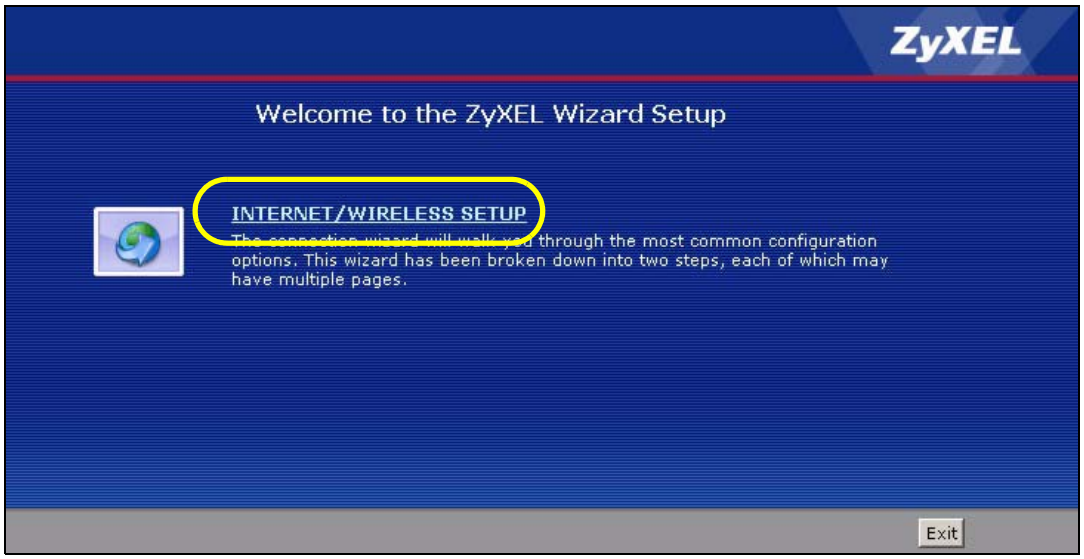
1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon in the top right corner of the Web Configurator to open to the wizard.

**Figure 9** Select a Mode

ZyXEL
Please select Wizard or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.
Use Advanced mode if you need access to more advanced features not included in Wizard mode.
Go to Wizard setup
Go to Advanced setup
Click here to always start with the Advanced setup.
Apply
Exit

2 Click **INTERNET SETUP** to configure the system for Internet access.

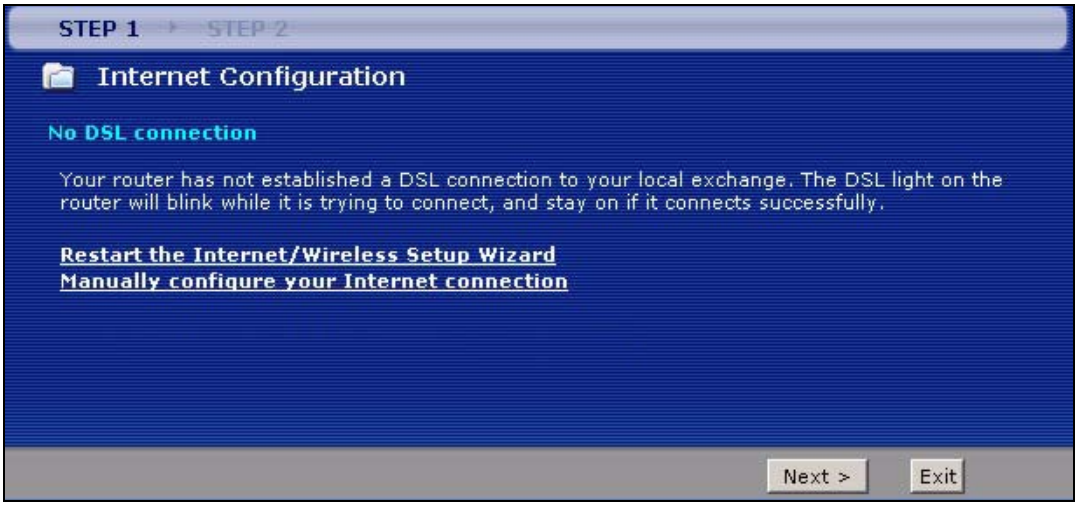
**Figure 10** Wizard Welcome


ZyXEL
Welcome to the ZyXEL Wizard Setup
INTERNET/WIRELESS SETUP
The connection wizard will walk you through the most common configuration options. This wizard has been broken down into two steps, each of which may have multiple pages.
Exit

3 Your ZyXEL device attempts to detect your DSL connection and your connection type.

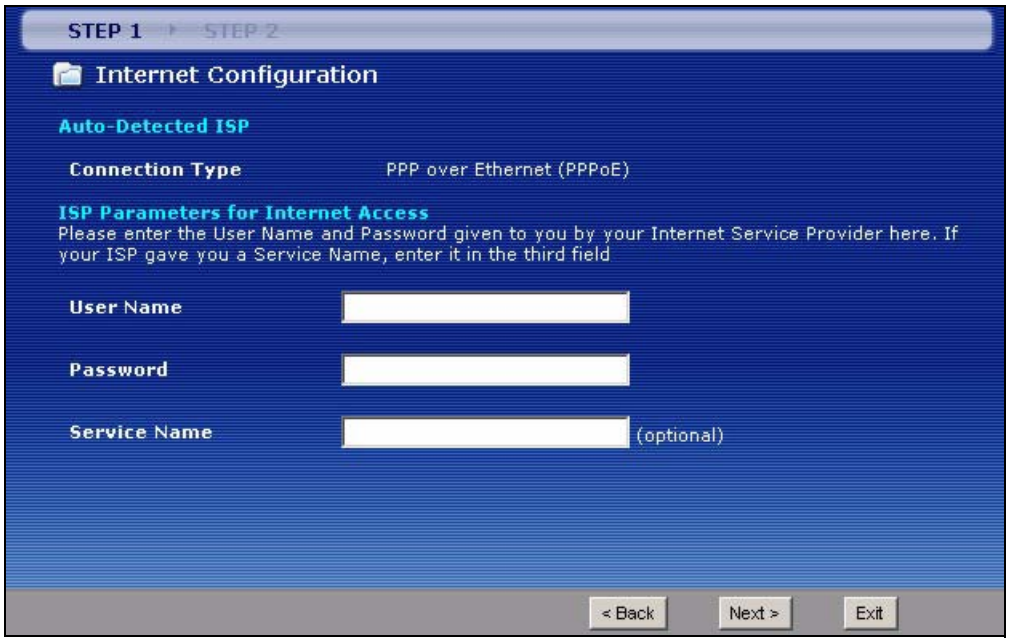
**3a** The following screen appears if a connection is not detected. Check your hardware connections and click **Restart the INTERNET SETUP Wizard** to return to the wizard welcome screen. If you still cannot connect, click **Manually configure your Internet connection**. Follow the directions in the wizard and enter your Internet setup information as provided to you by your ISP. See Section 5.2.1 on page 60 for more detail.

**Figure 11** Auto Detection: No DSL Connection


STEP 1
STEP 2
Internet Configuration
No DSL connection
Your router has not established a DSL connection to your local exchange. The DSL light on the router will blink while it is trying to connect, and stay on if it connects successfully.
Restart the Internet/Wireless Setup Wizard
Manually configure your Internet connection
Next >
Exit

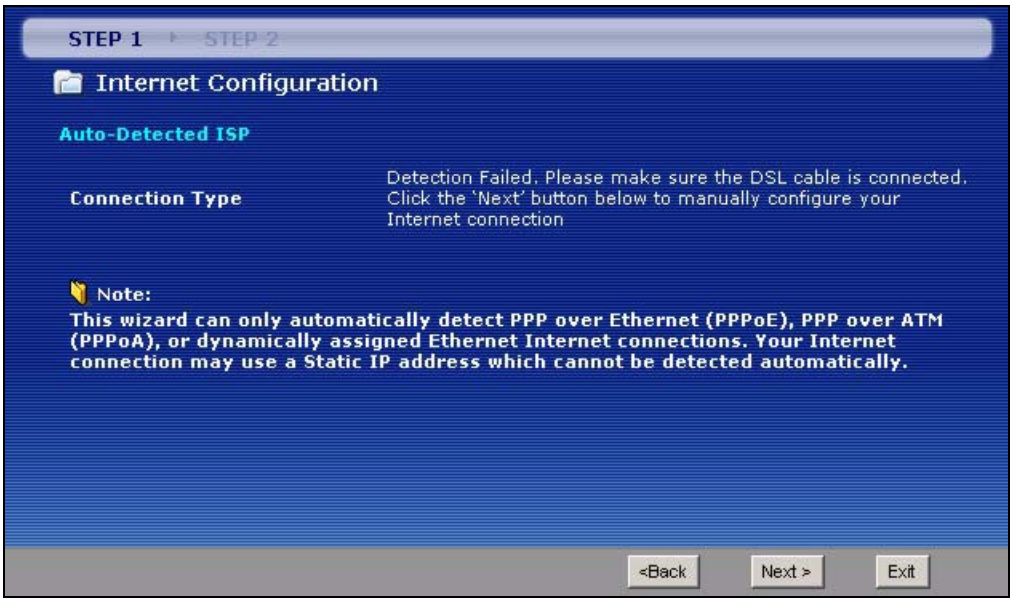
**3b** The following screen displays if a PPPoE or PPPoA connection is detected. Enter your Internet account information (username, password and/or service name) exactly as provided by your ISP. Then click **Next**.

**Figure 12** Auto-Detection: PPPoE


STEP 1
STEP 2
Internet Configuration
Auto-Detected ISP
Connection Type
PPP over Ethernet (PPPoE)
ISP Parameters for Internet Access
Please enter the User Name and Password given to you by your Internet Service Provider here. If your ISP gave you a Service Name, enter it in the third field
User Name
Password
Service Name
(optional)
< Back
Next >
Exit

**3c** The following screen appears if the ZyXEL device detects a connection but not the connection type. Click **Next** and refer to Section 5.2.1 on page 60 on how to manually configure the P-660H-T1v3s for Internet access.

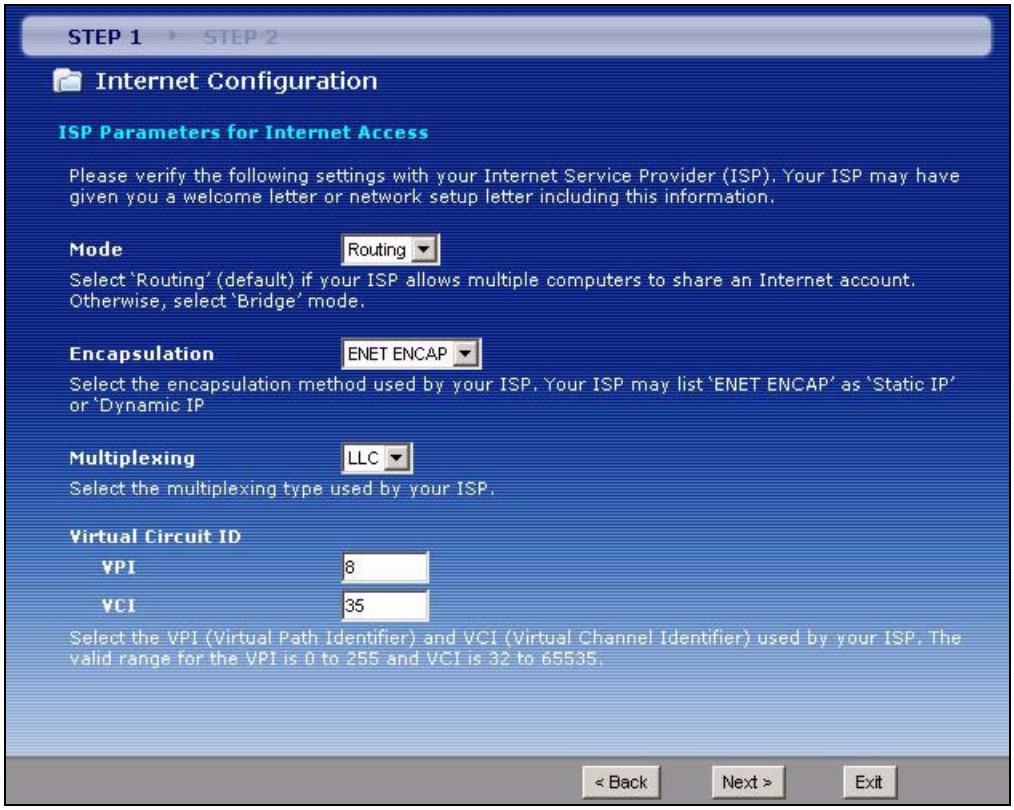
**Figure 13** Auto Detection: Failed


STEP 1
STEP 2
Internet Configuration
Auto-Detected ISP
Connection Type
Detection Failed. Please make sure the DSL cable is connected. Click the 'Next' button below to manually configure your Internet connection
Note:
This wizard can only automatically detect PPP over Ethernet (PPPoE), PPP over ATM (PPPoA), or dynamically assigned Ethernet Internet connections. Your Internet connection may use a Static IP address which cannot be detected automatically.
<Back
Next >
Exit

## 5.2.1 Manual Configuration

1 If the P-660H-T1v3s fails to detect your DSL connection type but the physical line is connected, enter your Internet access information in the wizard screen exactly as your service provider gave it to you. Leave the defaults in any fields for which you were not given information.

**Figure 14** Internet Access Wizard Setup: ISP Parameters


STEP 1
STEP 2
Internet Configuration
ISP Parameters for Internet Access
Please verify the following settings with your Internet Service Provider (ISP). Your ISP may have given you a welcome letter or network setup letter including this information.
Mode
Routing
Select 'Routing' (default) if your ISP allows multiple computers to share an Internet account. Otherwise, select 'Bridge' mode.
Encapsulation
ENET ENCAP
Select the encapsulation method used by your ISP. Your ISP may list 'ENET ENCAP' as 'Static IP' or 'Dynamic IP
Multiplexing
LLC
Select the multiplexing type used by your ISP.
Virtual Circuit ID
VPI
8
VCI
35
Select the VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) used by your ISP. The valid range for the VPI is 0 to 255 and VCI is 32 to 65535.
< Back
Next >
Exit

The following table describes the fields in this screen.

**Table 7** Internet Access Wizard Setup: ISP Parameters

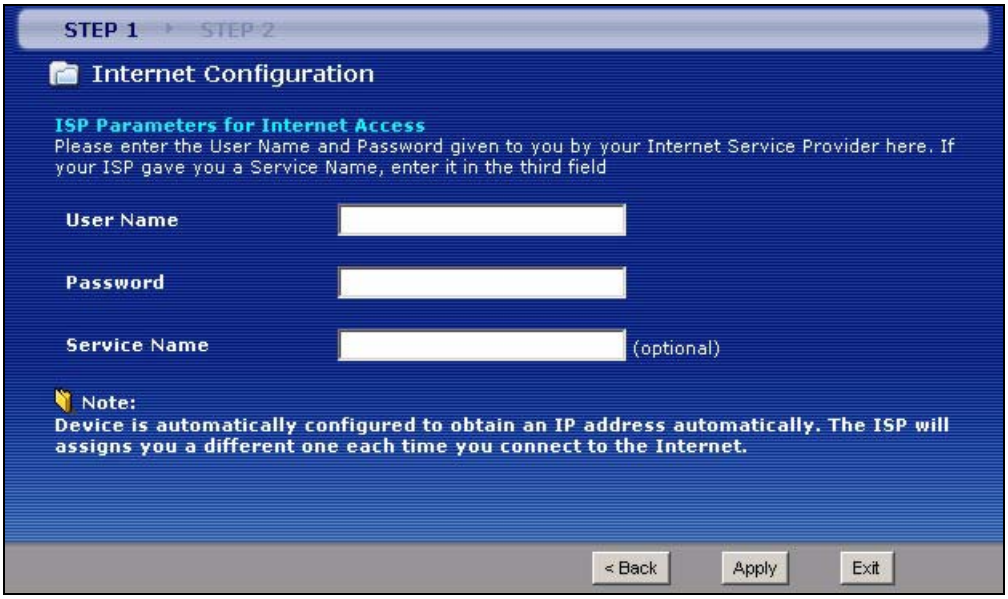
| LABEL | DESCRIPTION |
|---|---|
| Mode | Select **Routing** (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account. Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use Firewall, DHCP server and NAT on the P-660H-T1v3s. |
| Encapsulation | Select the encapsulation type your ISP uses from the **Encapsulation** drop-down list box. Choices vary depending on what you select in the **Mode** field.<br>If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**.<br>If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**. |

**Table 7** Internet Access Wizard Setup: ISP Parameters

| LABEL | DESCRIPTION |
|---|---|
| Multiplexing | Select the multiplexing method used by your ISP from the **Multiplex** drop-down list box either VC-based or LLC-based. |
| Virtual Circuit ID | VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information. |
| VPI | Enter the VPI assigned to you. This field may already be configured. |
| VCI | Enter the VCI assigned to you. This field may already be configured. |
| Back | Click this to return to the previous screen without saving. |
| Next | Click this to continue to the next wizard screen. The next wizard screen you see depends on what protocol you chose above. |
| Exit | Click this to close the wizard screen without saving. |

2 The next wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue.

**Figure 15** Internet Connection with PPPoE

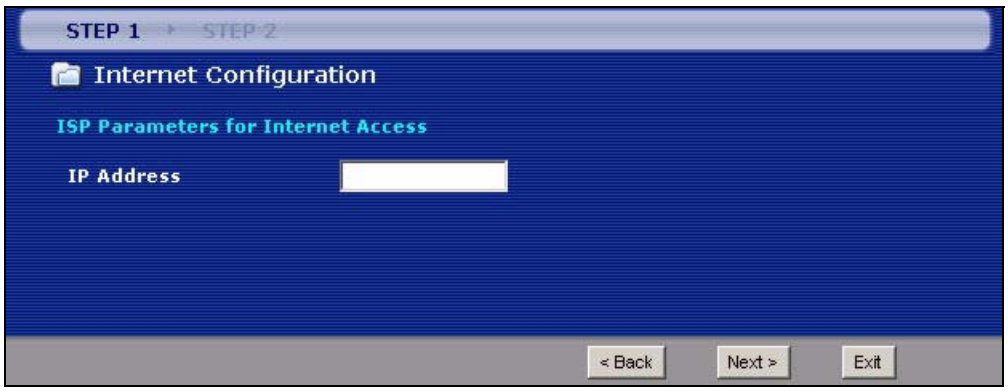

STEP 1
STEP 2
Internet Configuration
ISP Parameters for Internet Access
Please enter the User Name and Password given to you by your Internet Service Provider here. If your ISP gave you a Service Name, enter it in the third field
User Name
Password
Service Name
(optional)
Note:
Device is automatically configured to obtain an IP address automatically. The ISP will assigns you a different one each time you connect to the Internet.
< Back
Apply
Exit

The following table describes the fields in this screen.

**Table 8** Internet Connection with PPPoE

| LABEL | DESCRIPTION |
|---|---|
| User Name | Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given. |
| Password | Enter the password associated with the user name above. |
| Service Name | Type the name of your PPPoE service here. |
| Back | Click this to return to the previous screen without saving. |
| Apply | Click this to save your changes. |
| Exit | Click this to close the wizard screen without saving. |

**Figure 16** Internet Connection with RFC 1483

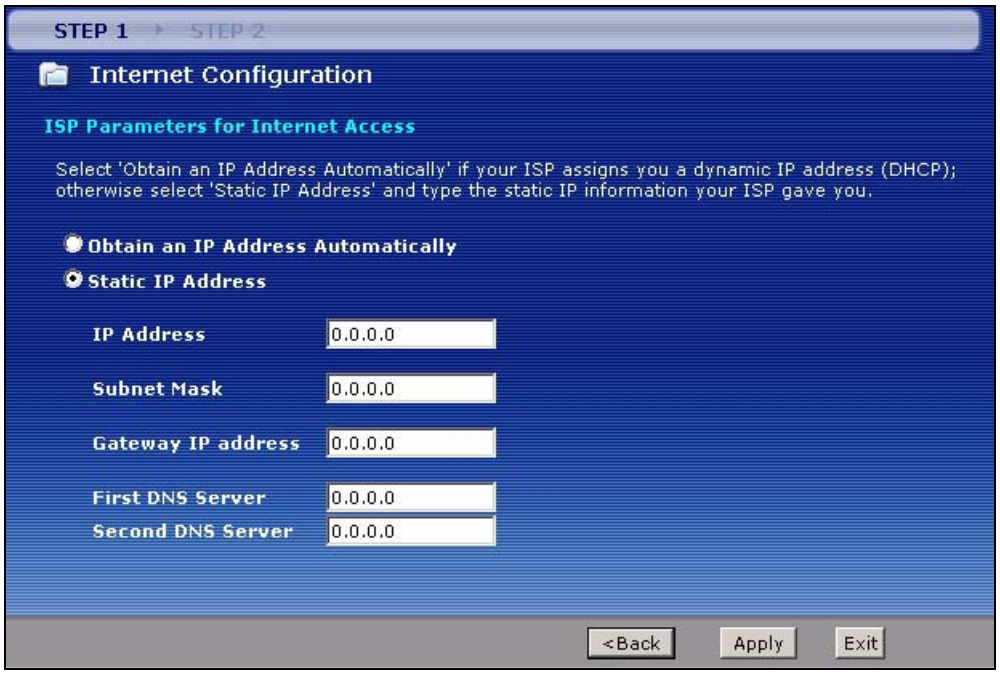


The following table describes the fields in this screen.

**Table 9** Internet Connection with RFC 1483

| LABEL | DESCRIPTION |
|---|---|
| IP Address | This field is available if you select **Routing** in the **Mode** field.<br>Type your ISP assigned IP address in this field. |
| Back | Click this to return to the previous screen without saving. |
| Next | Click this to continue to the next wizard screen. |
| Exit | Click this to close the wizard screen without saving. |

**Figure 17** Internet Connection with ENET ENCAP

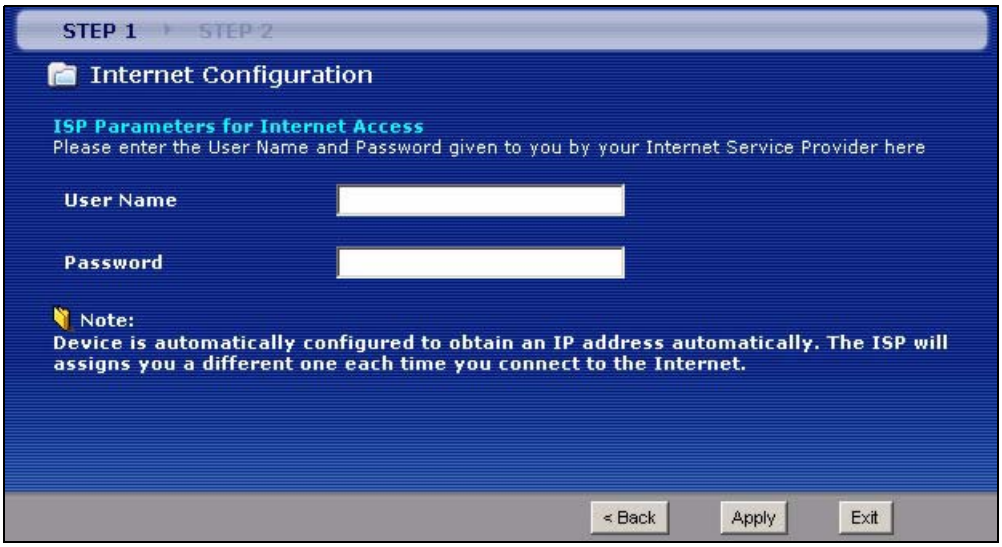


The following table describes the fields in this screen.

**Table 10** Internet Connection with ENET ENCAP

| LABEL | DESCRIPTION |
|---|---|
| Obtain an IP Address Automatically | A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.<br><br>Select **Obtain an IP Address Automatically** if you have a dynamic IP address. |
| Static IP Address | Select **Static IP Address** if your ISP gave you an IP address to use. |
| IP Address | Enter your ISP assigned IP address. |
| Subnet Mask | Enter a subnet mask in dotted decimal notation.<br><br>Refer to the appendix to calculate a subnet mask If you are implementing subnetting. |
| Gateway IP address | You must specify a gateway IP address (supplied by your ISP) when you use **ENET ENCAP** in the **Encapsulation** field in the previous screen. |
| First DNS Server | Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask. |
| Second DNS Server | As above. |
| Back | Click this to return to the previous screen without saving. |
| Apply | Click this to save your changes. |
| Exit | Click this to close the wizard screen without saving. |

**Figure 18** Internet Connection with PPPoA


STEP 1
STEP 2
Internet Configuration
ISP Parameters for Internet Access
Please enter the User Name and Password given to you by your Internet Service Provider here
User Name
Password
Note:
Device is automatically configured to obtain an IP address automatically. The ISP will assigns you a different one each time you connect to the Internet.
< Back
Apply
Exit

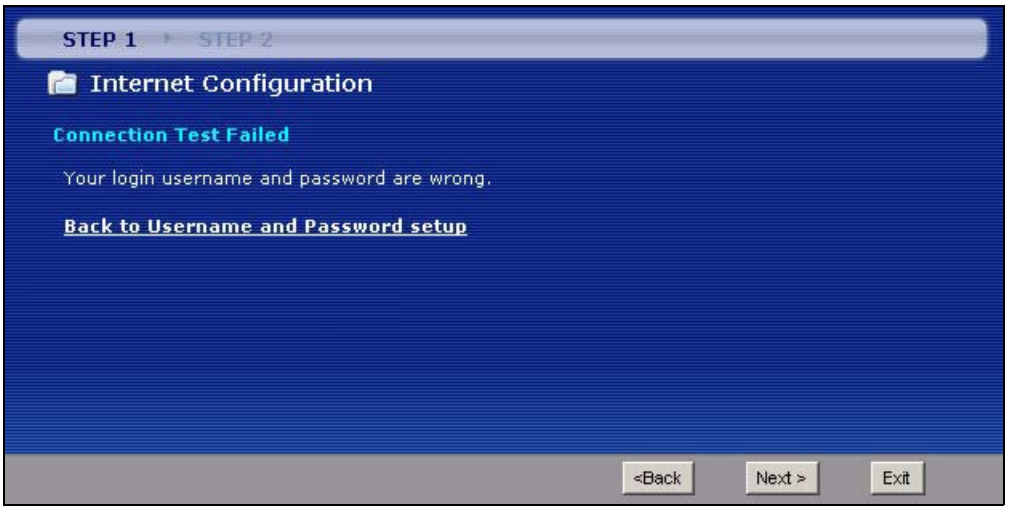
The following table describes the fields in this screen.

**Table 11** Internet Connection with PPPoA

| LABEL | DESCRIPTION |
|---|---|
| User Name | Enter the login name that your ISP gives you. |
| Password | Enter the password associated with the user name above. |
| Back | Click this to return to the previous screen without saving. |
| Apply | Click this to save your changes. |
| Exit | Click this to close the wizard screen without saving. |

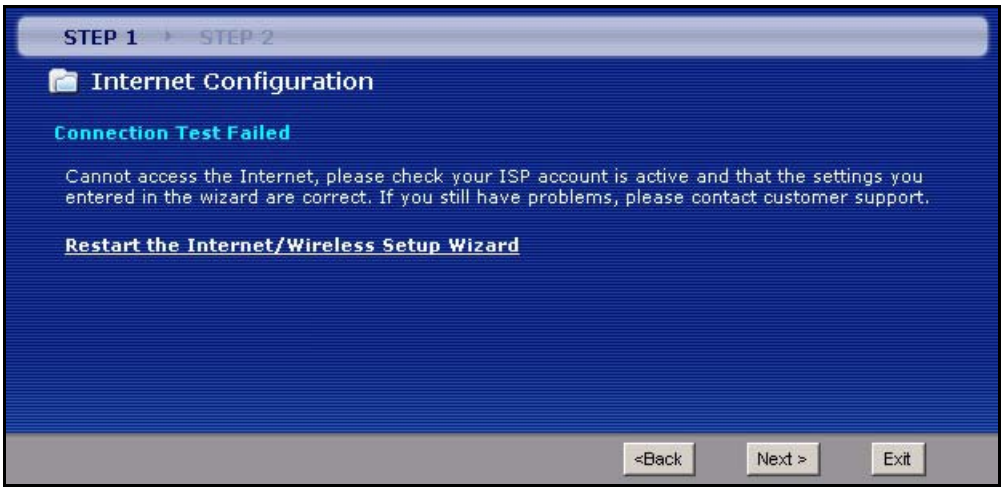
- If the user name and/or password you entered for PPPoE or PPPoA connection are not correct, the screen displays as shown next. Click **Back to Username and Password setup** to go back to the screen where you can modify them.

**Figure 19** Connection Test Failed-1




- If the following screen displays, check if your account is activated or click **Restart the Internet/Wireless Setup Wizard** to verify your Internet access settings.

**Figure 20** Connection Test Failed-2.


STEP 1
STEP 2
Internet Configuration
Connection Test Failed
Cannot access the Internet, please check your ISP account is active and that the settings you entered in the wizard are correct. If you still have problems, please contact customer support.
Restart the Internet/Wireless Setup Wizard
<Back
Next >
Exit

# PART II
# Technical Reference

# 6

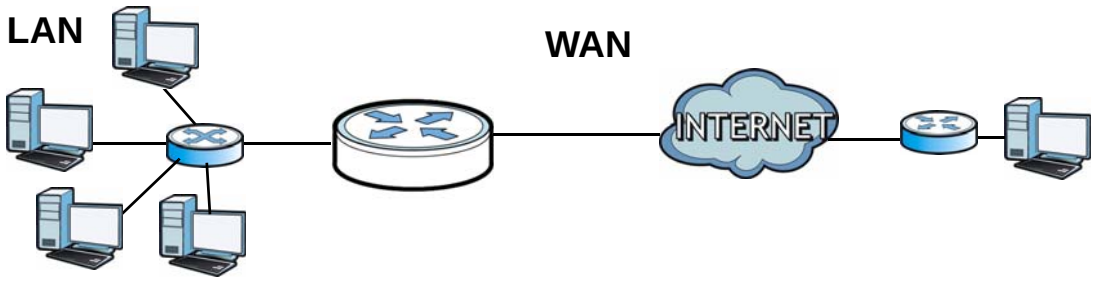
# WAN Setup

## 6.1 Overview

This chapter describes how to configure WAN settings from the **WAN** screens. Use these screens to configure your P-660H-T1v3s for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks (such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

**Figure 21** LAN and WANw




### 6.1.1 What You Can Do in the WAN Screens

- Use the **Internet Connection** screen (Section 6.2 on page 71) to configure the WAN settings on the P-660H-T1v3s for Internet access.
- Use the **More Connections** screen (Section 6.3 on page 77) to set up additional Internet access connections.

### 6.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

### Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPPoA, they should also provide a username and password (and service name) for user authentication.

### WAN IP Address

The WAN IP address is an IP address for the P-660H-T1v3s, which makes it accessible from an outside network. It is used by the P-660H-T1v3s to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the P-660H-T1v3s tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

### Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just one.

### IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 is still in wide use.

### Finding Out More

See Section 6.4 on page 82 for technical background information on WAN.

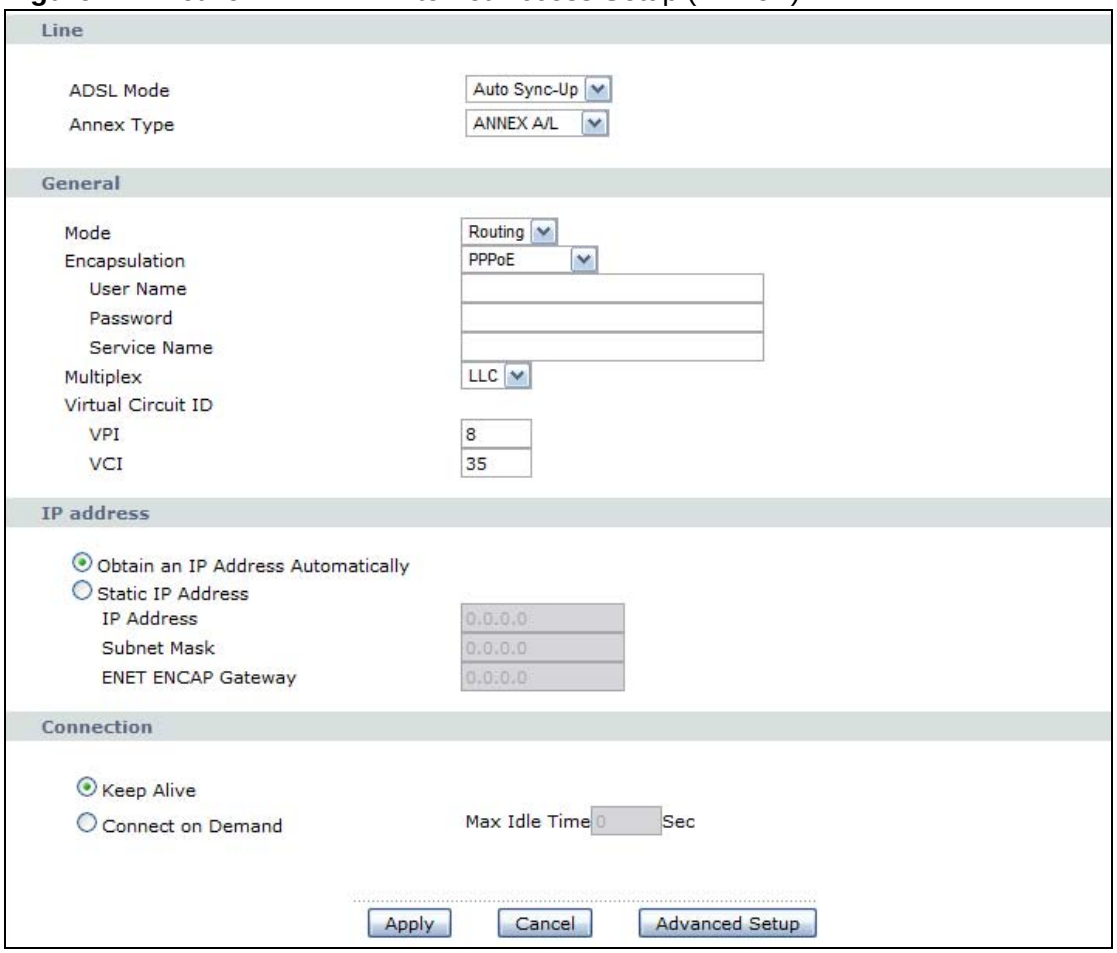
## 6.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

# 6.2 The Internet Access Setup Screen

Use this screen to change your P-660H-T1v3s's WAN settings. Click **Network > WAN > Internet Access Setup**. The screen differs by the WAN type and encapsulation you select.

**Figure 22** Network > WAN >Internet Access Setup (PPPoE)



The following table describes the labels in this screen.

**Table 12** Network > WAN > Internet Access Setup

| LABEL | DESCRIPTION |
|---|---|
| Line | |
| ADSL Mode | Select the modulation supported by your ISP.<br><br>Use **Auto Sync-Up** if you are not sure which mode to choose from. The P-660H-T1v3s dynamically diagnoses the mode supported by the ISP and selects the best compatible one for your connection.<br><br>Other options are: **ADSL2+**, **ADSL2, G.DMT**, **T1.413** and **G.lite**.<br><br>**ADSL2+**: This mode has a downstream rate of 24 Mbit/s and an upstream rate of 1.0 Mbit/s.<br><br>**ADSL2**: This mode has a downstream rate of 12 Mbit/s and an upstream rate of 1.0 Mbit/s.<br><br>**G.DMT**: This mode has a downstream rate of 12 Mbit/s and an upstream rate of 1.3 Mbit/s.<br><br>**T1.413**: This mode has downstream rate of 8 Mbit/s and an upstream rate of 1.0 Mbit/s.<br><br>**G.lite**: This mode has a downstream rate of 1.5 Mbit/s and an upstream rate of 0.5 Mbit/s. This type of DSL does not use splitter. |
| Annex Type | Select the annex type supported by your ISP. An annex defines how ADSL works under certain conditions.<br><br>Options are:<br><br>**Annex A** - This is ADSL over POTS (Plain Old Telephone Service), most commonly found in North America. It uses a frequency of 138 kHz.<br><br>**Annex A/L** - This is Reach Extended ADSL2 (READSL2), allowing an ISP to extend the distance data can be transmitted over Annex A by up to 7 kilometers. Because it has high power requirements that may result in audible cross-talk over lines, it sees limited deployment.<br><br>**Annex M** - This is an optional modification of Annex A that doubles the DSL device's upstream bits. It also shifts the frequency of Annex A up to 276 kHz.<br><br>**Annex A/L/M**-This is a combination of the A, L and M annexes. |
| General | |
| Mode | Select **Routing** (default) from the drop-down list box if your ISP gives you one IP address only and you want multiple computers to share an Internet account.<br><br>Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use Firewall, DHCP server and NAT on the P-660H-T1v3s. |

**Table 12** Network > WAN > Internet Access Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| Encapsulation | Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field.<br><br>**PPPoA** - Point-to-Point Protocol over ATM (PPPoA) encapsulates PPP frames inside ATM Adaptation Layer 5 frames. PPPoA is a similar specification to PPPoE and is used for for connecting users on an local network connection (such as from a computer to a routing device) to the Internet through a common broadband medium, such as a single DSL line or wireless device. However, this specification has slightly lower overhead than PPPoE as it has 2 less transport layers.<br><br>**RFC 1483** - Multiprotocol Encapsulation over ATM Adaptation Layer 5 allows an ATM virtual circuit to mimic the properties of an Ethernet IP LAN, connecting the two either through bridging or routing.<br><br>**ENET ENCAP** - The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instanced, it encapsulated routed Ethernet frames into bridged ATM cells.<br><br>**PPPoE** - Point-to-Point Protocol over Ethernet (PPPoE) encapsulates PPP frames inside Ethernet frames. PPPoE is a similar specification to PPPoA for connecting users on an local network connection (such as from a computer to a routing device) to the Internet through a common broadband medium, such as a single DSL line or wireless device. However, this specification has slightly higher overhead than PPPoA as it has 2 more transport layers. |
| User Name | (PPPoA and PPPoE encapsulation only.)<br><br>Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given. |
| Password | (PPPoA and PPPoE encapsulation only.)<br><br>Enter the password associated with the user name above. |
| Service Name | (PPPoE only.)<br><br>Type the name of your PPPoE service here. |
| Multiplex | Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.<br><br>This field is not available if you set the WAN type to **Ethernet**. |
| Virtual Circuit ID | VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.<br><br>These fields are not available if you set the WAN type to **Ethernet**. |
| VPI | The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. |
| VCI | The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you. |

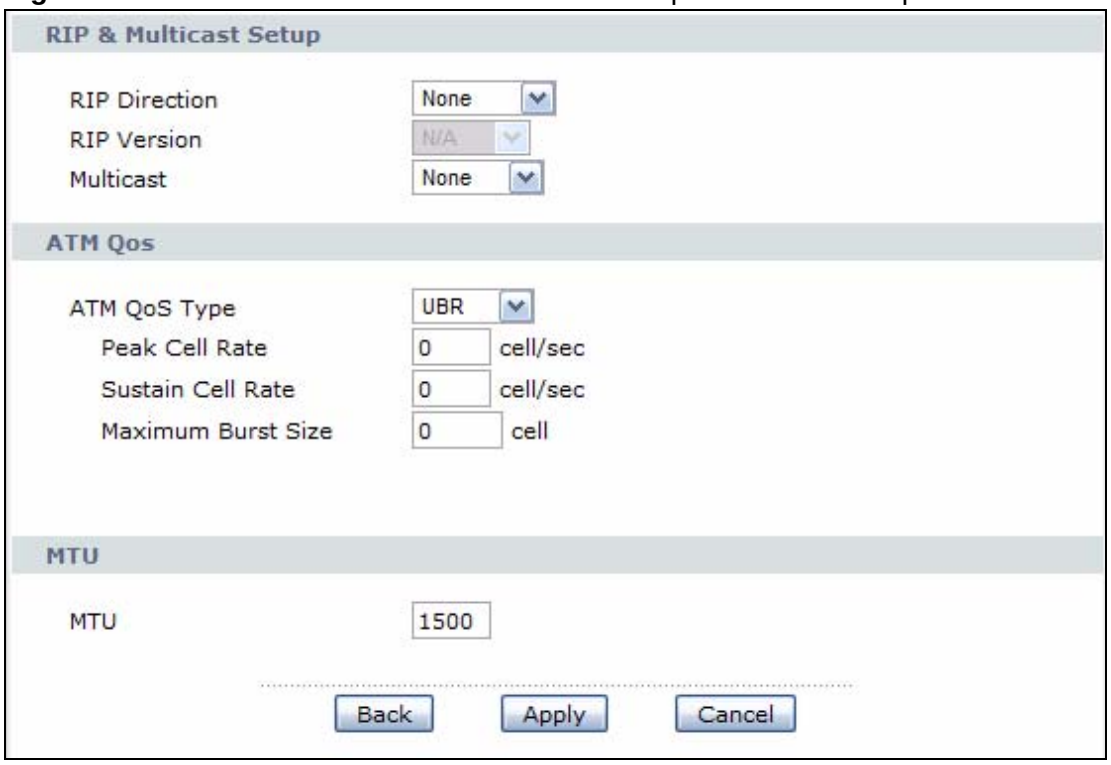
**Table 12** Network > WAN > Internet Access Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP Address | This option is available if you select **Routing** in the **Mode** field.<br><br>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.<br><br>Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below. |
| Subnet Mask | This option is available if you select **ENET ENCAP** in the **Encapsulation** field.<br><br>Enter a subnet mask in dotted decimal notation. |
| ENET ENCAP Gateway | This option is available if you select **ENET ENCAP** in the **Encapsulation** field.<br><br>Specify a gateway IP address (supplied by your ISP). |
| Connection (PPPoA and PPPoE encapsulation only.) | |
| Keep Alive | Select this when you want your connection up all the time. The P-660H-T1v3s will try to bring up the connection automatically if it is disconnected. |
| Connect on Demand | Select this when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field. |
| Max Idle Timeout | Specify an idle time-out in this field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |
| Advanced Setup | Click this to display the **Advanced WAN Setup** screen and edit more details of your WAN setup. |

## 6.2.1 Advanced Internet Access Setup

Use this screen to edit your P-660H-T1v3s's advanced WAN settings. Click the **Advanced Setup** button in the **Internet Access Setup** screen. The screen appears as shown.

**Figure 23** Network > WAN > Internet Access Setup: Advanced Setup




The following table describes the labels in this screen.

**Table 13** Network > WAN > Internet Access Setup: Advanced Setup

| LABEL | DESCRIPTION |
|---|---|
| RIP & Multicast Setup | This section is not available when you configure the P-660H-T1v3s to be in bridge mode. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Use this field to control how much routing information the P-660H-T1v3s sends and receives on the subnet.<br><br>Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**. |
| RIP Version | This field is not configurable if you select **None** in the **RIP Direction** field.<br><br>Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**. |

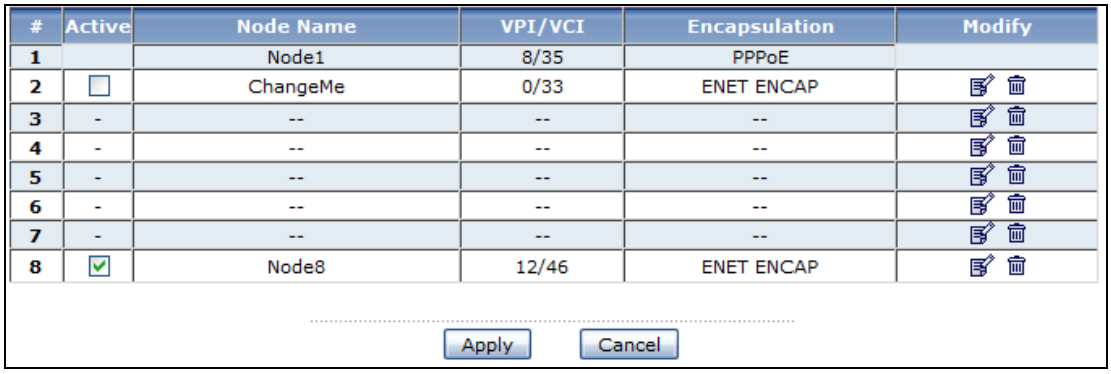
**Table 13** Network > WAN > Internet Access Setup: Advanced Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| Multicast | Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).<br><br>Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a multicast group. The P-660H-T1v3s supports **IGMP-v1**, **IGMP-v2** and **IGMP-v3**. Select **None** to disable it. |
| ATM QoS | |
| ATM QoS Type | Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR-RT** (real-time Variable Bit Rate) type for applications with bursty connections that require closely controlled delay and delay variation. Select **VBR-nRT** (non real-time Variable Bit Rate) type for connections that do not require closely controlled delay and delay variation. |
| Peak Cell Rate | Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here. |
| Sustain Cell Rate | The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. |
| Maximum Burst Size | Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. |
| MTU | |
| MTU | The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field.<br><br>For ENET ENCAP, the MTU value is 1500.<br><br>For PPPoE, the MTU value is 1492.<br><br>For PPPoA and RFC 1483, the MTU is 65535. |
| Back | Click this to return to the previous screen without saving. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 6.3 The More Connections Screen

The P-660H-T1v3s allows you to configure more than one Internet access connection. To configure additional Internet access connections click **Network > WAN > More Connections**. The screen differs by the encapsulation you select. When you use the **WAN > Internet Access Setup** screen to set up Internet access, you are configuring the first WAN connection.

**Figure 24** Network > WAN > More Connections




The following table describes the labels in this screen.

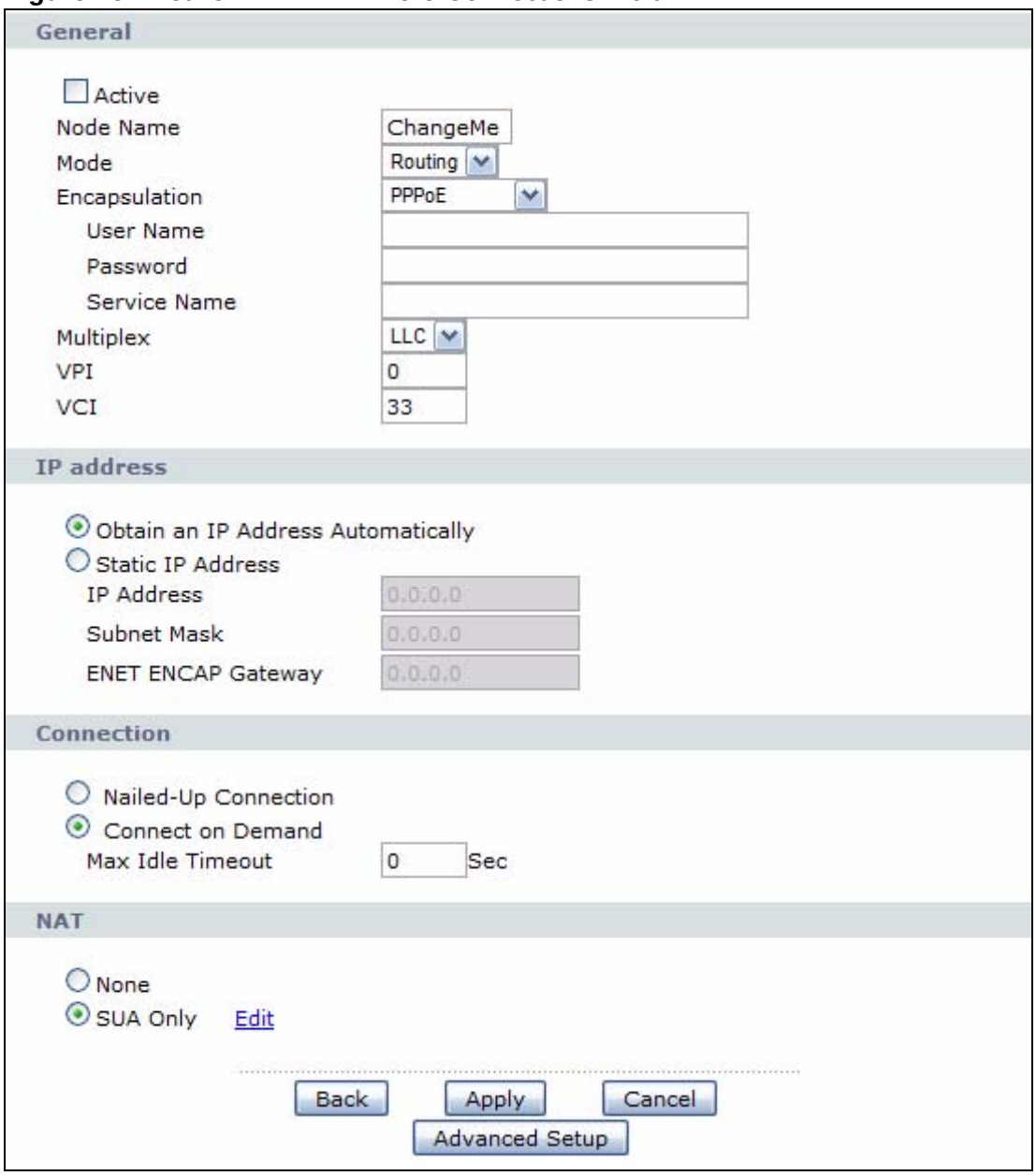
**Table 14** Network > WAN > More Connections

| LABEL | DESCRIPTION |
|---|---|
| # | This is an index number indicating the number of the corresponding connection. |
| Active | This field indicates whether the connection is active or not.<br><br>Clear the check box to disable the connection. Select the check box to enable it. |
| Node Name | This is the name you gave to the Internet connection. |
| VPI/VCI | This field displays the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers configured for this WAN connection. |
| Encapsulation | This field indicates the encapsulation method of the Internet connection. |
| Modify | The first (ISP) connection is read-only in this screen. Use the **WAN > Internet Access Setup** screen to edit it.<br><br>Click the **Edit** icon to edit the Internet connection settings. Click this icon on an empty configuration to add a new Internet access setup.<br><br>Click the **Remove** icon to delete the Internet access setup from your connection list. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

## 6.3.1 More Connections Edit

Use this screen to configure a connection. Click the edit icon in the **More Connections** screen to display the following screen.

**Figure 25** Network > WAN > More Connections: Edit



The following table describes the labels in this screen.

**Table 15** Network > WAN > More Connections: Edit

| LABEL | DESCRIPTION |
|---|---|
| General | |
| Active | Select the check box to activate or clear the check box to deactivate this connection. |
| Node Name | Enter a unique, descriptive name of up to 13 ASCII characters for this connection. |
| Mode | Select **Routing** from the drop-down list box if your ISP allows multiple computers to share an Internet account.<br><br>If you select **Bridge**, the P-660H-T1v3s will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. |
| Encapsulation | Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field.<br><br>If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**.<br><br>If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**. |
| User Name | (PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given. |
| Password | (PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above. |
| Service Name | (PPPoE only) Type the name of your PPPoE service here. |
| Multiplex | Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.<br><br>By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol.<br><br>For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols. |
| VPI | The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. |
| VCI | The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you. |

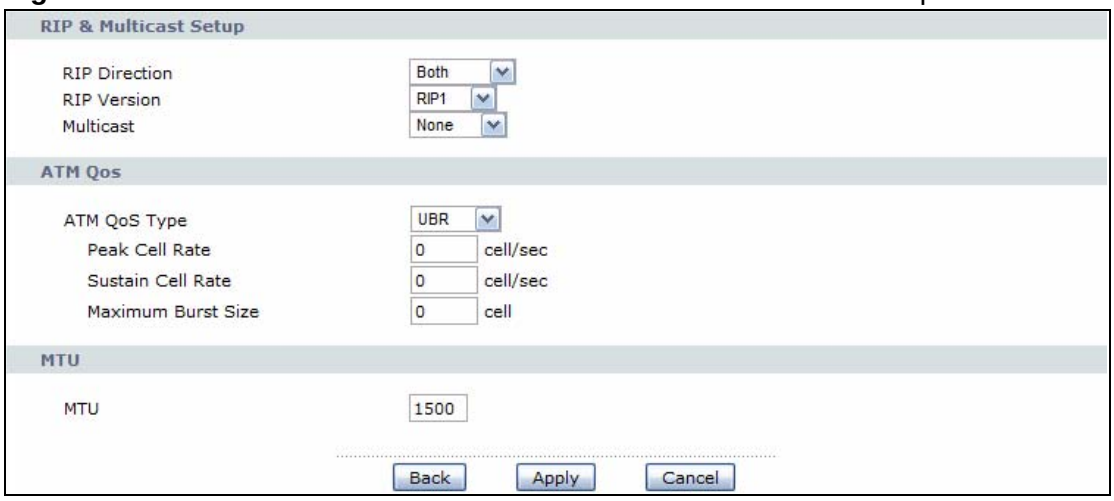
**Table 15** Network > WAN > More Connections: Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP Address | This option is available if you select **Routing** in the **Mode** field.<br><br>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.<br><br>If you use the encapsulation type except **RFC 1483**, select **Obtain an IP Address Automatically** when you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below.<br><br>If you use **RFC 1483**, enter the IP address given by your ISP in the **IP Address** field. |
| Subnet Mask | This option is available if you select **ENET ENCAP** in the **Encapsulation** field.<br><br>Enter a subnet mask in dotted decimal notation. |
| ENET ENCAP Gateway | This option is available if you select **ENET ENCAP** in the **Encapsulation** field.<br><br>Specify a gateway IP address (supplied by your ISP). |
| Connection | |
| Nailed-Up Connection | Select **Nailed-Up Connection** when you want your connection up all the time. The P-660H-T1v3s will try to bring up the connection automatically if it is disconnected. |
| Connect on Demand | Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field. |
| Max Idle Timeout | Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout. |
| NAT | **SUA only** is available only when you select **Routing** in the **Mode** field.<br><br>Select **SUA Only** if you have one public IP address and want to use NAT. Click **Edit** to go to the **Port Forwarding** screen to edit a server mapping set.<br><br>Otherwise, select **None** to disable NAT. |
| Back | Click this to return to the previous screen without saving. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |
| Advanced Setup | Click this to display the **More Connections Advanced Setup** screen and edit more details of your WAN setup. |

## 6.3.2 Configuring More Connections Advanced Setup

Use this screen to edit your P-660H-T1v3s's advanced WAN settings. Click the **Advanced Setup** button in the **More Connections Edit** screen. The screen appears as shown.

**Figure 26** Network > WAN > More Connections: Edit: Advanced Setup




The following table describes the labels in this screen.

**Table 16** Network > WAN > More Connections: Edit: Advanced Setup

| LABEL | DESCRIPTION |
|---|---|
| RIP & Multicast Setup | This section is not available when you configure the P-660H-T1v3s to be in bridge mode. |
| RIP Direction | Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**. |
| RIP Version | Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**. |
| Multicast | IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The P-660H-T1v3s supports **IGMP-v1**, **IGMP-v2** and **IGMP-v3**. Select **None** to disable it. |
| ATM QoS | |
| ATM QoS Type | Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR-nRT** (Variable Bit Rate-non Real Time) or **VBR-RT** (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications. |
| Peak Cell Rate | Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here. |
| Sustain Cell Rate | The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. |

**Table 16** Network > WAN > More Connections: Edit: Advanced Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| Maximum Burst Size | Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. |
| MTU | |
| MTU | The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field.<br>For ENET ENCAP, the MTU value is 1500.<br>For PPPoE, the MTU value is 1492.<br>For PPPoA and RFC, the MTU is 65535. |
| Back | Click this to return to the previous screen without saving. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 6.4 WAN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

## 6.4.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The P-660H-T1v3s supports the following methods.

### 6.4.1.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells.

### 6.4.1.2 PPP over Ethernet

The P-660H-T1v3s supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The PPPoE option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the P-660H-T1v3s (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-660H-T1v3s does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

#### 6.4.1.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The P-660H-T1v3s encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (Digital Subscriber Line (DSL) Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

#### 6.4.1.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

### 6.4.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

**VC-based Multiplexing**

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

### LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

## 6.4.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

## 6.4.4 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

### IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **Gateway IP Address** fields are not applicable (N/A). If you have a static IP, then you only need to fill in the **IP Address** field and not the **Gateway IP Address** field.

### IP Assignment with RFC 1483 Encapsulation

In this case the IP address assignment must be static.

### IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **Gateway IP Address** fields as supplied by your ISP. However for a dynamic IP, the P-660H-T1v3s acts as a DHCP client on the WAN port and so the **IP Address** and **Gateway IP Address** fields are not applicable (N/A) as the DHCP server assigns them to the P-660H-T1v3s.

## 6.4.5 Keep Alive/Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The P-660H-T1v3s does two things when you specify

a nailed-up connection. The first is that idle timeout is disabled. The second is that the P-660H-T1v3s will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

### 6.4.6 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

## 6.5 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

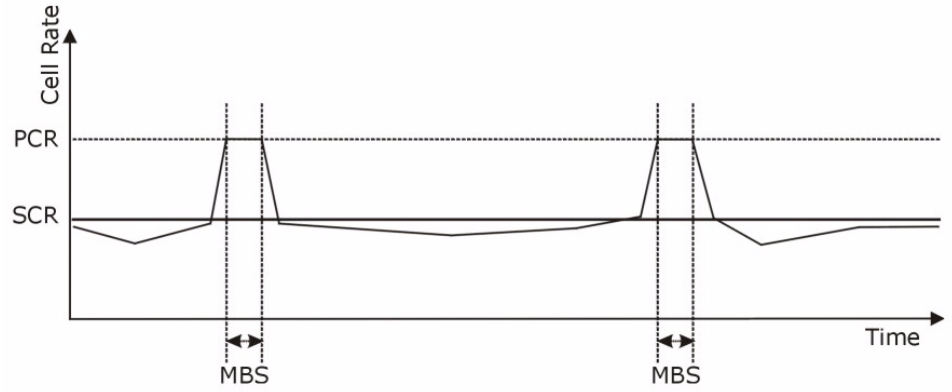
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

**Figure 27** Example of Traffic Shaping




## 6.5.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

### Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

### Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst

levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

### Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

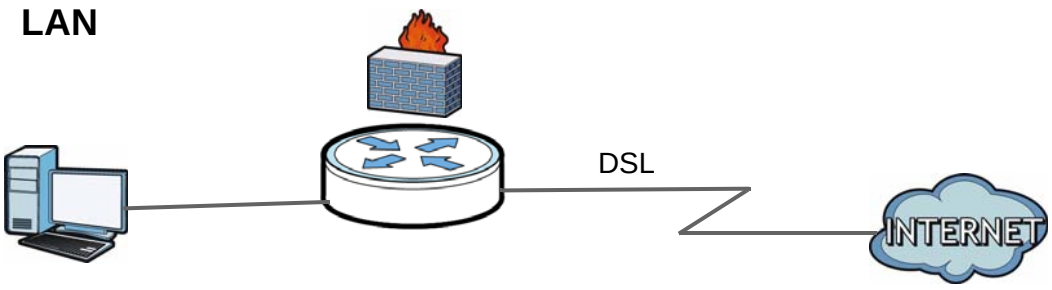
# 7

# LAN Setup

## 7.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one immediate area such as a building or floor of a building.

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.




### 7.1.1 What You Can Do in the LAN Screens

- Use the **IP** screen (Section 7.2 on page 91) to set the LAN IP address and subnet mask of your ZyXEL device. You can also edit your P-660H-T1v3s's RIP, multicast, any IP and Windows Networking settings from this screen.
- Use the **DHCP Setup** screen (Section 7.3 on page 93) to configure the ZyXEL Device's DHCP settings.
- Use the **Client List** screen (Section 7.4 on page 94) to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.
- Use the **IP Alias** screen (Section 7.5 on page 96) to change your P-660H-T1v3s's IP alias settings.

### 7.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

### IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

### Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

### DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your P-660H-T1v3s an IP address, subnet mask, DNS and other routing information when it's turned on.

### RIP

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.

### Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

### IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 is still in wide use.

### DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it.

### Finding Out More

See Section 7.6 on page 98 for technical background information on LANs.

## 7.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

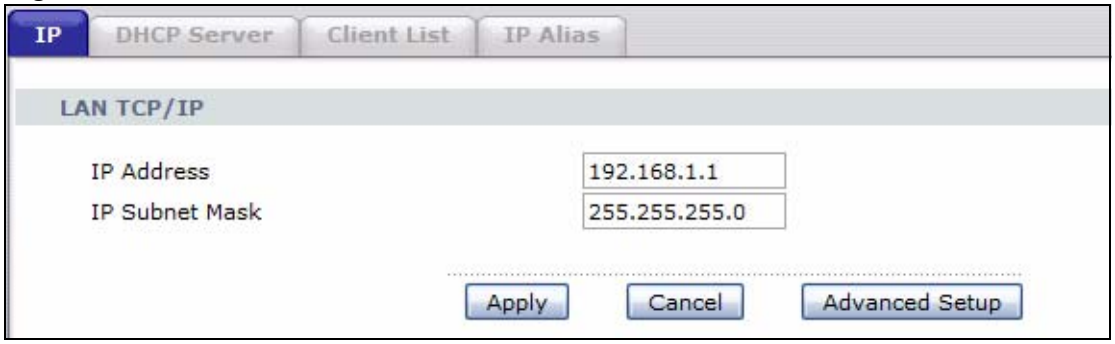
# 7.2 The IP Screen

Use this screen to set the Local Area Network IP address and subnet mask of your P-660H-T1v3s. Click **Network > LAN** to open the **IP** screen.

Follow these steps to configure your LAN settings.

1. Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your P-660H-T1v3s.
2. Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.
3. Click **Apply** to save your settings.

**Figure 28** Network > LAN > IP



The following table describes the fields in this screen.

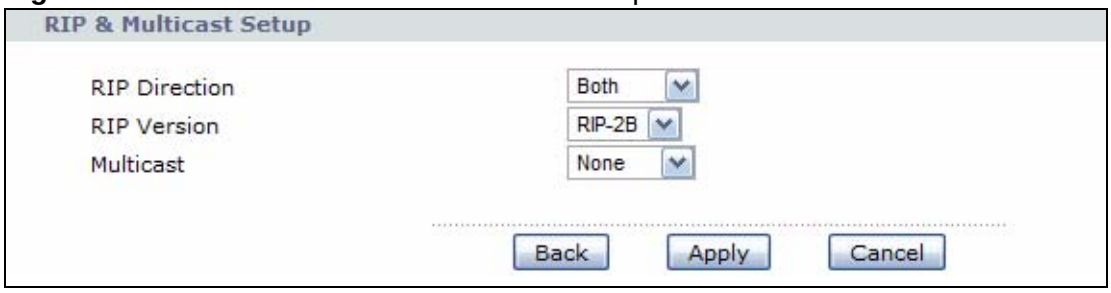
**Table 17** Network > LAN > IP

| LABEL | DESCRIPTION |
|---|---|
| IP Address | Enter the LAN IP address you want to assign to your P-660H-T1v3s in dotted decimal notation, for example, 192.168.1.1 (factory default). |
| IP Subnet Mask | Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your P-660H-T1v3s automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |
| Advanced Setup | Click this to display the **Advanced LAN Setup** screen and edit more details of your LAN setup. |

## 7.2.1 The Advanced LAN IP Setup Screen

Use this screen to edit your P-660H-T1v3s's RIP, multicast, Any IP and Windows Networking settings. Click the **Advanced Setup** button in the **LAN IP** screen. The screen appears as shown.

**Figure 29** Network > LAN > IP: Advanced Setup




The following table describes the labels in this screen.

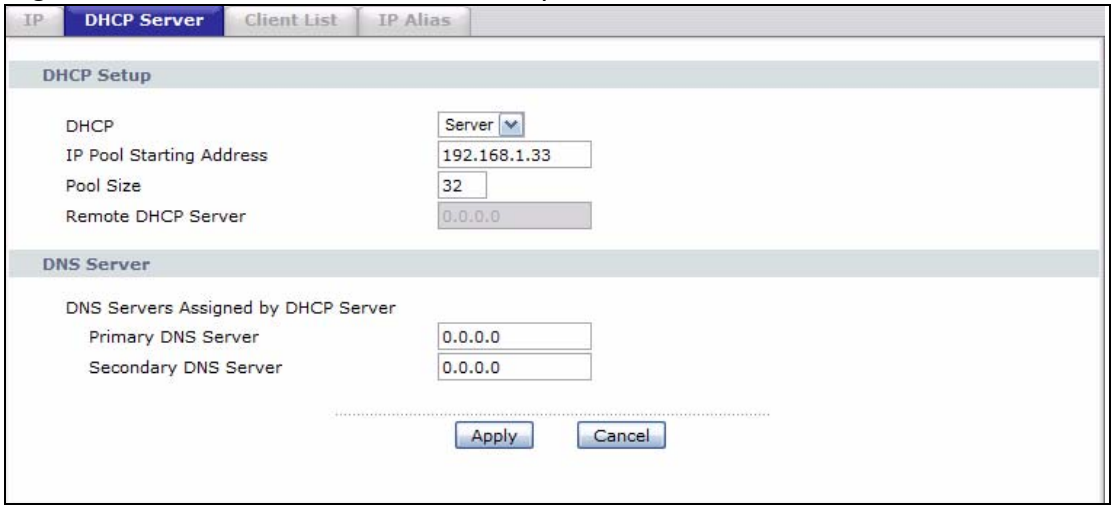
**Table 18** Network > LAN > IP: Advanced Setup

| LABEL | DESCRIPTION |
|---|---|
| RIP & Multicast Setup | |
| RIP Direction | Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**. |
| RIP Version | Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**. |
| Multicast | IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The P-660H-T1v3s supports **IGMP-v1**, **IGMP-v2** and **IGMP-v3**. Select **None** to disable it. |
| Back | Click this to return to the previous screen without saving. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 7.3 The DHCP Setup Screen

Use this screen to configure the DNS server information that the P-660H-T1v3s sends to the DHCP client devices on the LAN. Click **Network > DHCP Setup** to open this screen.

**Figure 30** Network > LAN > DHCP Setup




The following table describes the labels in this screen.

**Table 19** Network > LAN > DHCP Setup

| LABEL | DESCRIPTION |
|---|---|
| DHCP Setup | |
| DHCP | If set to **Server**, your P-660H-T1v3s can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.<br>If set to **None**, the DHCP server will be disabled.<br>If set to **Relay**, the P-660H-T1v3s acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** field in this case.<br>When DHCP is used, the following items need to be set: |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| Remote DHCP Server | If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here. |
| DNS Server | |
| DNS Servers Assigned by DHCP Server | The P-660H-T1v3s passes a DNS (Domain Name System) server IP address to the DHCP clients. |

**Table 19** Network > LAN > DHCP Setup

| LABEL | DESCRIPTION |
|---|---|
| First DNS Server<br>Second DNS Server | Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the P-660H-T1v3s's WAN IP address).<br><br>Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**.<br><br>Select **DNS Relay** to have the P-660H-T1v3s act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The P-660H-T1v3s's LAN IP address displays in the field to the right (read-only). The P-660H-T1v3s tells the DHCP clients on the LAN that the P-660H-T1v3s itself is the DNS server. When a computer on the LAN sends a DNS query to the P-660H-T1v3s, the P-660H-T1v3s forwards the query to the real DNS server learned through IPCP and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**.<br><br>Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

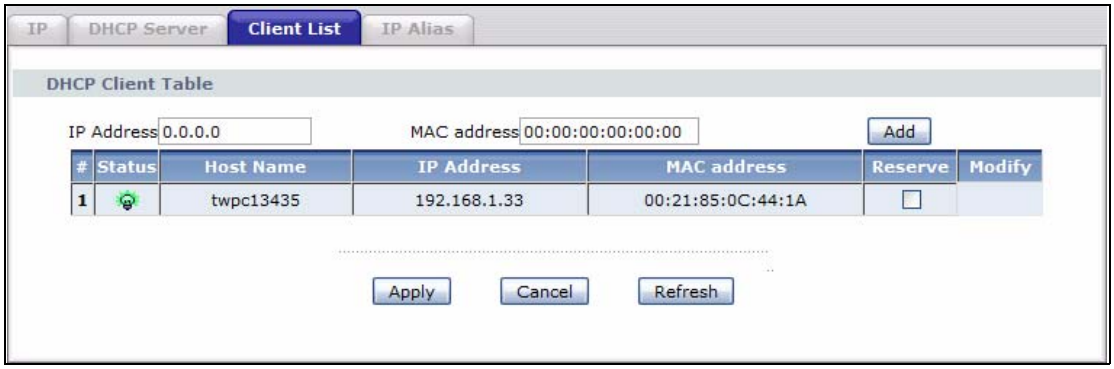
# 7.4 The Client List Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Use this screen to change your P-660H-T1v3s's static DHCP settings. Click **Network > LAN > Client List** to open the following screen.

**Figure 31** Network > LAN > Client List




The following table describes the labels in this screen.

**Table 20** Network > LAN > Client List

| LABEL | DESCRIPTION |
|---|---|
| IP Address | Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify. |
| MAC Address | Enter the MAC address of a computer on your LAN. |
| Add | Click this to add a static DHCP entry. |
| # | This is the index number of the static IP table entry (row). |
| Status | This field displays whether the client is connected to the P-660H-T1v3s. |
| Host Name | This field displays the computer host name. |
| IP Address | This field displays the IP address relative to the # field listed above. |
| MAC Address | The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation).<br><br>A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address. |
| Reserve | Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the P-660H-T1v3s always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 10 entries in this table. |
| Modify | Click the modify icon to have the IP address field editable and change it. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |
| Refresh | Click this to reload the DHCP table. |

# 7.5 The IP Alias Screen

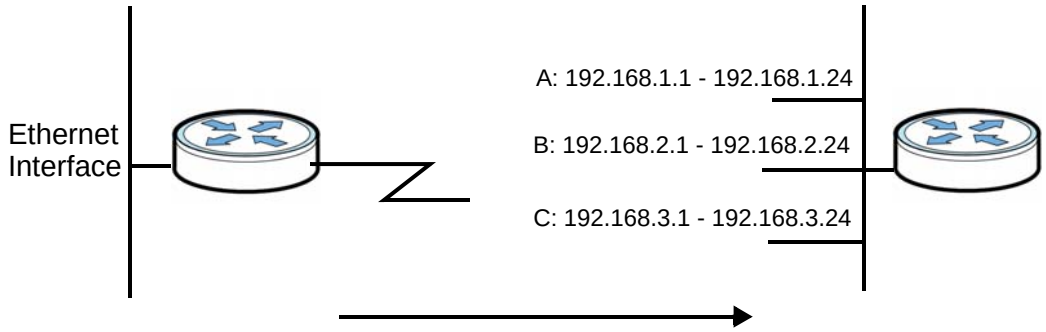
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The P-660H-T1v3s supports three logical LAN interfaces via its single physical Ethernet interface with the P-660H-T1v3s itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Note: Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A, B, and C.

**Figure 32** Physical Network & Partitioned Logical Networks




## 7.5.1 Configuring the LAN IP Alias Screen

Use this screen to change your P-660H-T1v3s's IP alias settings. Click **Network** > **LAN** > **IP Alias** to open the following screen.

**Figure 33** Network > LAN > IP Alias

The following table describes the labels in this screen.

**Table 21** Network > LAN > IP Alias

| LABEL | DESCRIPTION |
|---|---|
| IP Alias 1 | Select the check box to configure another LAN network for the P-660H-T1v3s. |
| IP Address | Enter the IP address of your P-660H-T1v3s in dotted decimal notation. |
| IP Subnet Mask | Your P-660H-T1v3s will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the P-660H-T1v3s. |
| RIP Direction | RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both/In Only/Out Only/None**. When set to **Both** or **Out Only**, the P-660H-T1v3s will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the P-660H-T1v3s sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

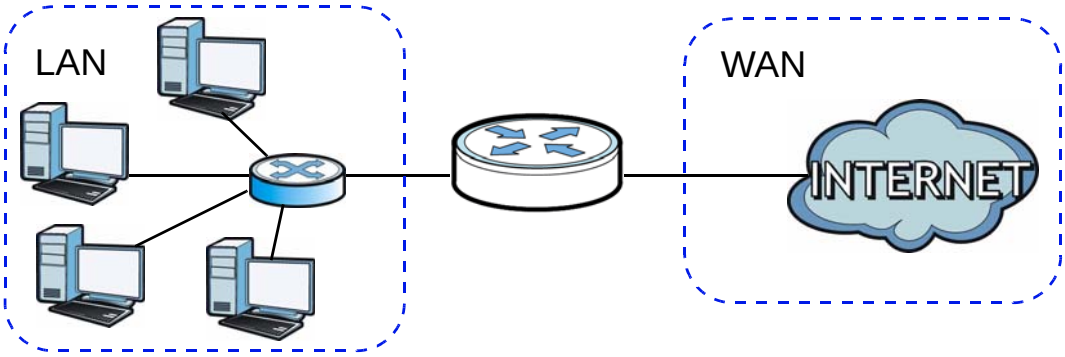
# 7.6 LAN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

## 7.6.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the P-660H-T1v3s ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

**Figure 34** LAN and WAN IP Addresses




## 7.6.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the P-660H-T1v3s as a DHCP server or disable it. When configured as a server, the P-660H-T1v3s provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

### IP Pool Setup

The P-660H-T1v3s is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

## 7.6.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The P-660H-T1v3s supports the IPCP DNS server extensions through the DNS proxy feature.

  If the **DNS Server** fields in the **DHCP Setup** screen are set to **DNS Relay**, the P-660H-T1v3s tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the P-660H-T1v3s, the P-660H-T1v3s acts as a DNS proxy and forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

## 7.6.4 LAN TCP/IP

The P-660H-T1v3s has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

### IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the

Network Address Translation (NAT) feature of the P-660H-T1v3s. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your P-660H-T1v3s, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your P-660H-T1v3s will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-660H-T1v3s unless you are instructed to do otherwise.

### Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

## 7.6.5 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both -** the P-660H-T1v3s will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only -** the P-660H-T1v3s will not send any RIP packets but will accept all RIP packets received.
- **Out Only -** the P-660H-T1v3s will send out RIP packets but will not accept any RIP packets received.
- **None -** the P-660H-T1v3s will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the P-660H-T1v3s sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

## 7.6.6 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The P-660H-T1v3s supports IGMP version 1 (**IGMP-v1**), IGMP version 2 (**IGMP-v2**) and IGMP version 3 (**IGMP-v3**). At start up, the P-660H-T1v3s queries all directly connected networks to gather group membership. After that, the P-660H-T1v3s periodically updates this information. IP multicasting can be enabled/ disabled on the P-660H-T1v3s LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

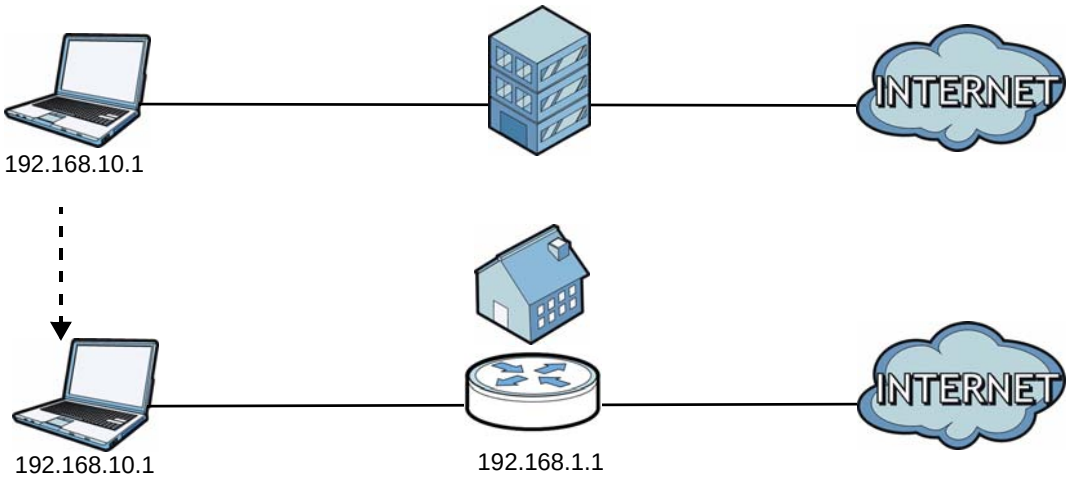
## 7.6.7 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the P-660H-T1v3s to be in the same subnet to allow the computer to access the Internet (through the P-660H-T1v3s). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the P-660H-T1v3s.

With the Any IP feature and NAT enabled, the P-660H-T1v3s allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the P-660H-T1v3s are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the P-660H-T1v3s and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a P-660H-T1v3s is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the P-660H-T1v3s are not in the same subnet.

**Figure 35** Any IP Example



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the P-660H-T1v3s's IP address.

Note: You must enable NAT/SUA to use the Any IP feature on the P-660H-T1v3s.

### How Any IP Works

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the P-660H-T1v3s) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the P-660H-T1v3s.

1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the P-660H-T1v3s) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
3. The P-660H-T1v3s receives the ARP request and replies to the computer with its own MAC address.
4. The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the P-660H-T1v3s.
5. When the P-660H-T1v3s receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

   After all the routing information is updated, the computer can access the P-660H-T1v3s and the Internet as if it is in the same subnet as the P-660H-T1v3s.

# 8

# Network Address Translation (NAT)

## 8.1 Overview

This chapter discusses how to configure NAT on the P-660H-T1v3s. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

### 8.1.1 What You Can Do in the NAT Screens

- Use the **NAT General Setup** screen (Section 8.2 on page 107) to configure the NAT setup settings.
- Use the **Port Forwarding** screen (Section 8.3 on page 108) to configure forward incoming service requests to the server(s) on your local network.
- Use the **Address Mapping** screen (Section 8.4 on page 112) to change your P-660H-T1v3s's address mapping settings.
- Use the **SIP ALG** screen (Section 8.5 on page 115) to enable and disable the SIP (VoIP) ALG in the P-660H-T1v3s.

### 8.1.2 What You Need To Know About NAT

#### Inside/Outside

Inside/outside denotes where a host is located relative to the P-660H-T1v3s, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

#### Global/Local

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

### NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

### Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

### SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The P-660H-T1v3s also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in Table 29 on page 119.

- Choose **SUA Only** if you have just one public WAN IP address for your P-660H-T1v3s.
- Choose **Full Feature** if you have multiple public WAN IP addresses for your P-660H-T1v3s.

### Finding Out More

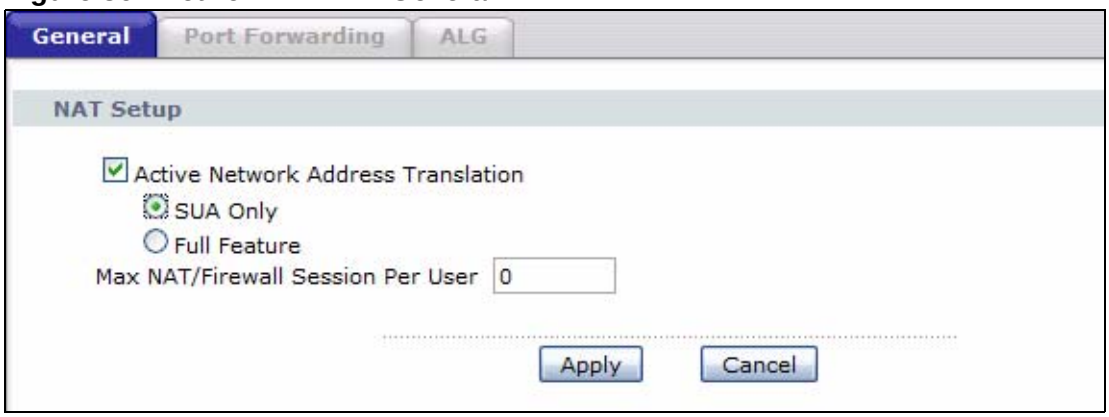
See Section 8.6 on page 116 for advanced technical information on NAT.

# 8.2 The NAT General Setup Screen

Use this screen to activate NAT. Click **Network > NAT** to open the following screen.

Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the P-660H-T1v3s.

**Figure 36** Network > NAT > General




The following table describes the labels in this screen.

**Table 22** Network > NAT > General

| LABEL | DESCRIPTION |
|---|---|
| Active Network Address Translation (NAT) | Select this check box to enable NAT. |
| SUA Only | Select this radio button if you have just one public WAN IP address for your P-660H-T1v3s. |
| Full Feature | Select this radio button if you have multiple public WAN IP addresses for your P-660H-T1v3s. |
| Max NAT/ Firewall Session Per User | When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.<br><br>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/Firewall sessions client computers can establish through the P-660H-T1v3s.<br><br>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is exhausting all of the available NAT sessions. |

**Table 22** Network > NAT > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 8.3 The Port Forwarding Screen

Note: This screen is available only when you select **SUA only** in the **NAT > General** screen.

Use this screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

The most often used port numbers and services are shown in Appendix D on page 255. Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

### Default Server IP Address

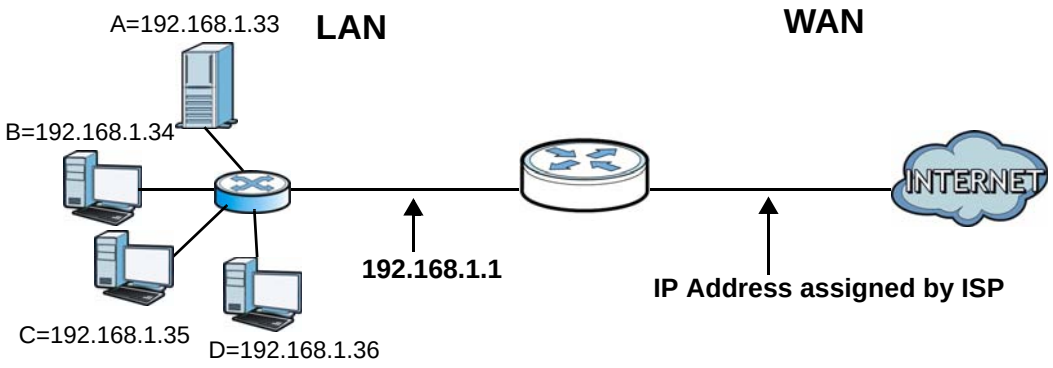
In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

Note: If you do not assign a **Default Server** IP address, the P-660H-T1v3s discards all packets received for ports that are not specified here or in the remote management setup.

### Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

**Figure 37** Multiple Servers Behind NAT Example

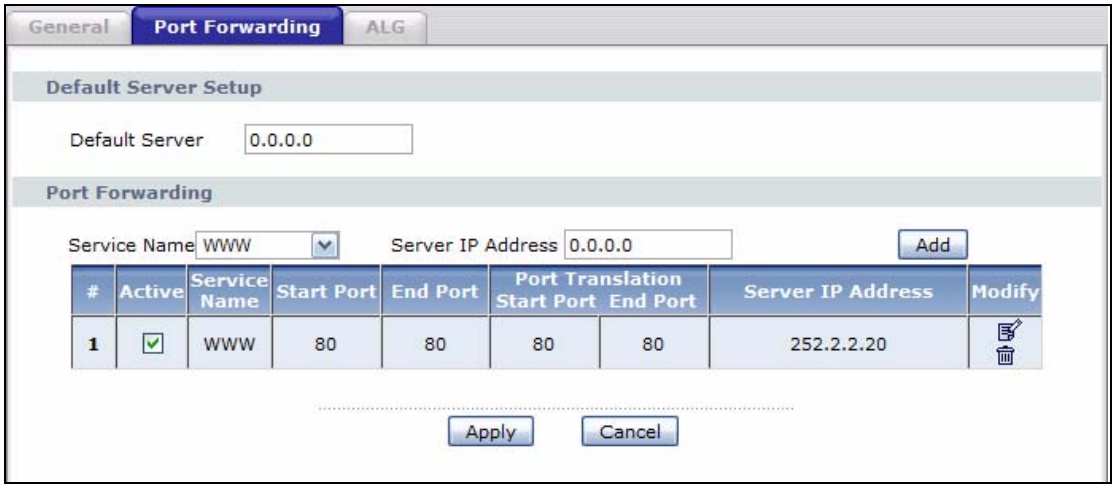



## 8.3.1 Configuring the Port Forwarding Screen

Click **Network > NAT > Port Forwarding** to open the following screen.

See Appendix D on page 255 for port numbers commonly used for particular services.

**Figure 38** Network > NAT > Port Forwarding



The following table describes the fields in this screen.

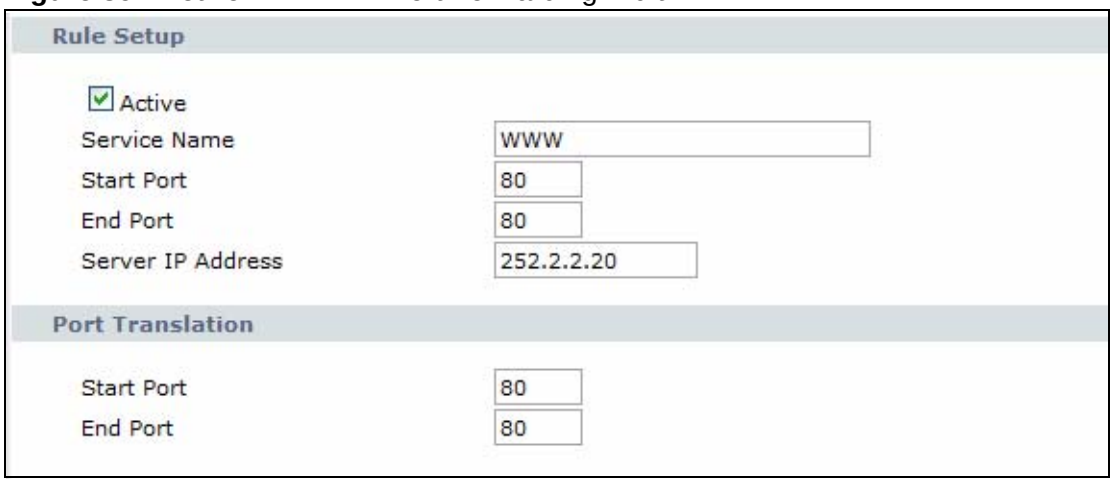
**Table 23** Network > NAT > Port Forwarding

| LABEL | DESCRIPTION |
|---|---|
| Default Server Setup | |
| Default Server | In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the P-660H-T1v3s discards all packets received for ports that are not specified here or in the remote management setup. |
| Port Forwarding | |
| Service Name | Select a service from the drop-down list box. |
| Server IP Address | Enter the IP address of the server for the specified service. |
| Add | Click this button to add a rule to the table below. |
| # | This is the rule index number (read-only). |
| Active | This field indicates whether the rule is active or not.<br>Clear the check box to disable the rule. Select the check box to enable it. |
| Service Name | This is a service's name. |
| Start Port | This is the first port number that identifies a service. |
| End Port | This is the last port number that identifies a service. |
| Port Translation Start Port | This is the first port number that identifies the range of ports managed by the port address translation service. |
| Port Translation End Port | This is the last port number that identifies the range of ports managed by the port address translation service. |
| Server IP Address | This is the server's IP address. |
| Modify | Click the edit icon to go to the screen where you can edit the port forwarding rule.<br>Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

## 8.3.2 The Port Forwarding Rule Edit Screen

Use this screen to edit a port forwarding rule. Click the rule's edit icon in the **Port Forwarding** screen to display the screen shown next.

**Figure 39** Network > NAT > Port Forwarding: Edit




The following table describes the fields in this screen.

**Table 24** Network > NAT > Port Forwarding: Edit

| LABEL | DESCRIPTION |
|---|---|
| Rule Setup | |
| Active | Click this check box to enable the rule. |
| Service Name | Enter a name to identify this port-forwarding rule. |
| Start Port | Enter a port number in this field.<br>To forward only one port, enter the port number again in the **End Port** field.<br>To forward a series of ports, enter the start port number here and the end port number in the **End Port** field. |
| End Port | Enter a port number in this field.<br>To forward only one port, enter the port number again in the **Start Port** field above and then enter it again in this field.<br>To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above. |
| Server IP Address | Enter the inside IP address of the server here. |
| Port Translation | |
| Start Port | This is the first port number that identifies the range of ports managed by the port address translation service. |
| End Port | This is the last port number that identifies the range of ports managed by the port address translation service. |
| Back | Click this to return to the previous screen without saving. |

**Table 24** Network > NAT > Port Forwarding: Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

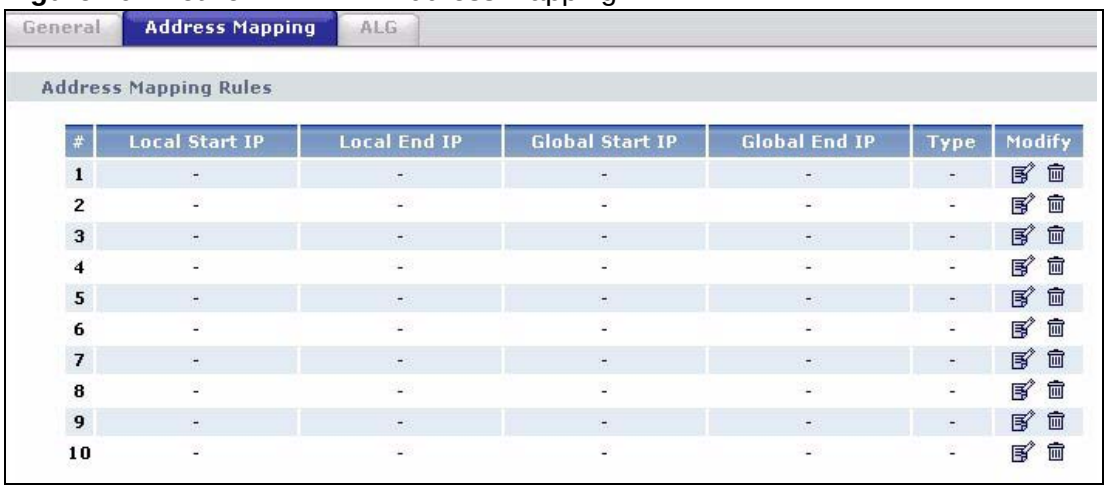
# 8.4 The Address Mapping Screen

Note: The **Address Mapping** screen is available only when you select **Full Feature** in the **NAT > General** screen.

Ordering your rules is important because the P-660H-T1v3s applies the rules in the order that you specify. When a rule matches the current packet, the P-660H-T1v3s takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your P-660H-T1v3s's address mapping settings, click **Network > NAT > Address Mapping** to open the following screen.

**Figure 40** Network > NAT > Address Mapping


General
Address Mapping
ALG
Address Mapping Rules
# Local Start IP Local End IP Global Start IP Global End IP Type Modify
1 - - - - -
2 - - - - -
3 - - - - -
4 - - - - -
5 - - - - -
6 - - - - -
7 - - - - -
8 - - - - -
9 - - - - -
10 - - - - -

The following table describes the fields in this screen.

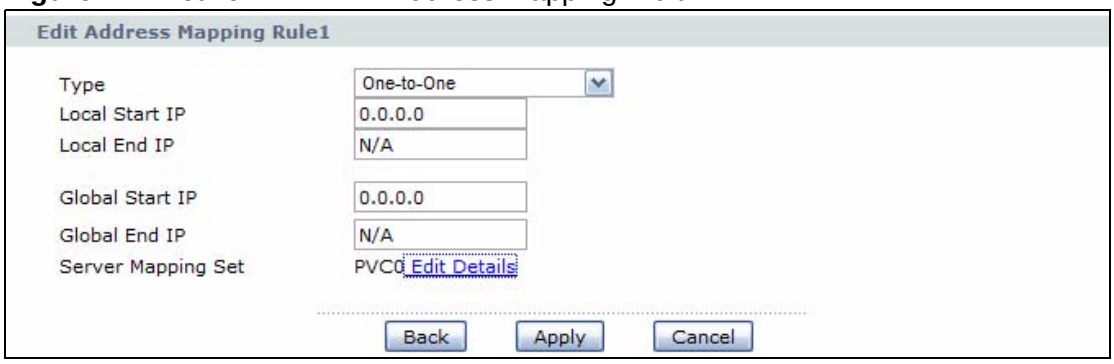
**Table 25** Network > NAT > Address Mapping

| LABEL | DESCRIPTION |
|---|---|
| # | This is the rule index number. |
| Local Start IP | This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types. |
| Global Start IP | This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types. |
| Global End IP | This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types. |
| Type | **1-1**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.<br><br>**M-1**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.<br><br>**M-M Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.<br><br>**MM No** (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.<br><br>**Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Modify | Click the edit icon to go to the screen where you can edit the address mapping rule.<br><br>Click the delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action. |

## 8.4.1 The Address Mapping Rule Edit Screen

Use this screen to edit an address mapping rule. Click the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

**Figure 41** Network > NAT > Address Mapping: Edit




The following table describes the fields in this screen.

**Table 26** Network > NAT > Address Mapping: Edit

| LABEL | DESCRIPTION |
|---|---|
| Type | Choose the port mapping type from one of the following.<br><br>**One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.<br><br>**Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.<br><br>**Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.<br><br>**Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.<br><br>**Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Local Start IP | This is the starting local IP address (ILA). Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address.<br><br>This field is **N/A** for **One-to-One** and **Server** mapping types. |
| Global Start IP | This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. |
| Global End IP | This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types. |

**Table 26** Network > NAT > Address Mapping: Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Server Mapping Set | Only available when **Type** is set to **Server**.<br>Select a number from the drop-down menu to choose a port forwarding set. |
| Edit Details | Click this link to go to the **Port Forwarding** screen to edit a port forwarding set that you have selected in the **Server Mapping Set** field. |
| Back | Click this to return to the previous screen without saving. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 8.5 The SIP ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the P-660H-T1v3s registers with the SIP register server, the SIP ALG translates the P-660H-T1v3s's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your P-660H-T1v3s is behind a SIP ALG.

Use this screen to enable and disable the SIP (VoIP) ALG in the P-660H-T1v3s. To access this screen, click **Network > NAT > ALG**.

**Figure 42** Network > NAT > ALG

The following table describes the fields in this screen.

**Table 27** Network > NAT > ALG

| LABEL | DESCRIPTION |
|---|---|
| Enable SIP ALG | Select this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules. |
| Apply | Click this to save your changes. |
| Reset | Click this to restore your previously saved settings. |

# 8.6 NAT Technical Reference

This chapter contains more information regarding NAT.

## 8.6.1 NAT Definitions

Inside/outside denotes where a host is located relative to the P-660H-T1v3s, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

**Table 28** NAT Definitions

| ITEM | DESCRIPTION |
|---|---|
| Inside | This refers to the host on the LAN. |
| Outside | This refers to the host on the WAN. |
| Local | This refers to the packet address (source or destination) as the packet travels on the LAN. |
| Global | This refers to the packet address (source or destination) as the packet travels on the WAN. |

NAT never changes the IP address (either local or global) of an outside host.

## 8.6.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

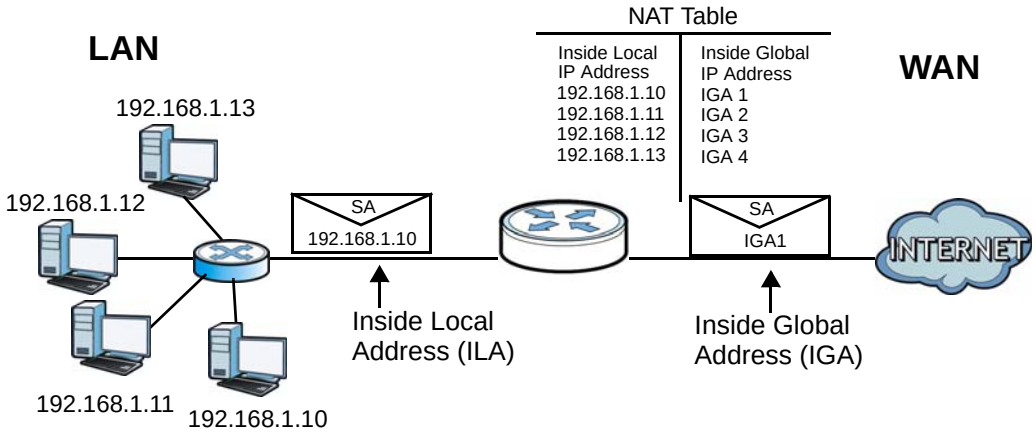
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the

outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see Table 29 on page 119), NAT offers the additional benefit of firewall protection. With no servers defined, your P-660H-T1v3s filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

## 8.6.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The P-660H-T1v3s keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

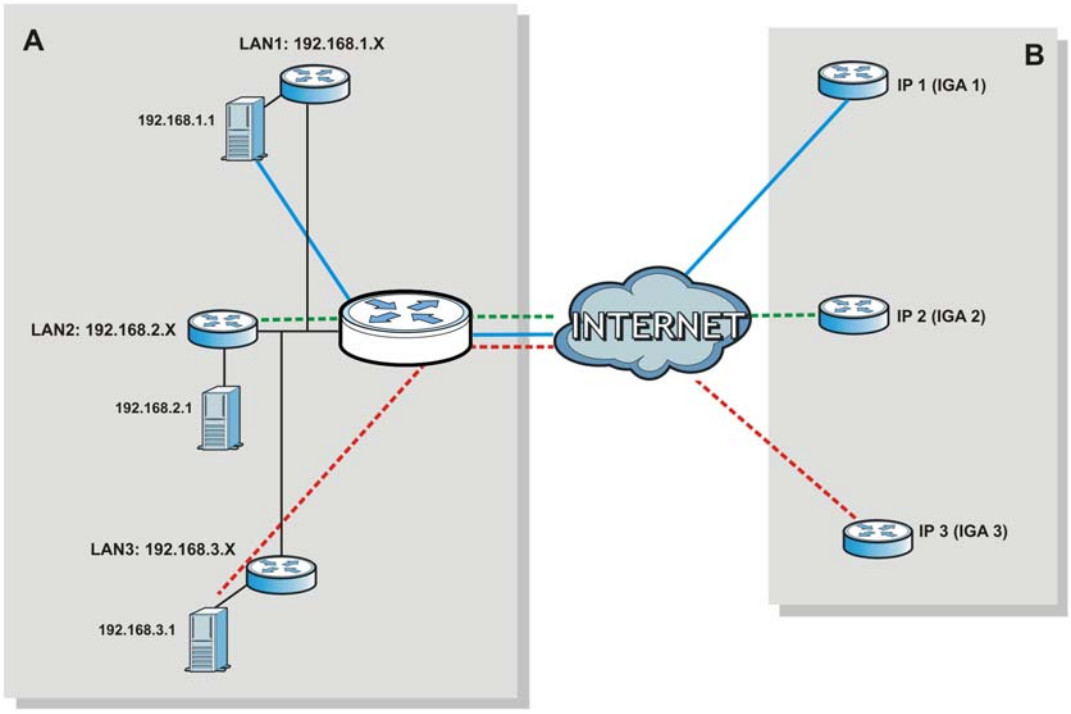
**Figure 43** How NAT Works



## 8.6.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the P-660H-T1v3s can communicate with three distinct WAN networks.

**Figure 44** NAT Application With IP Alias




## 8.6.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the P-660H-T1v3s maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the P-660H-T1v3s maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload**: In Many-to-Many Overload mode, the P-660H-T1v3s maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the P-660H-T1v3s maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

**Table 29** NAT Mapping Types

| TYPE | IP MAPPING |
|---|---|
| One-to-One | ILA1←→ IGA1 |
| Many-to-One (SUA/PAT) | ILA1←→ IGA1<br>ILA2←→ IGA1<br>... |
| Many-to-Many Overload | ILA1←→ IGA1<br>ILA2←→ IGA2<br>ILA3←→ IGA1<br>ILA4←→ IGA2<br>... |
| Many-to-Many No Overload | ILA1←→ IGA1<br>ILA2←→ IGA2<br>ILA3←→ IGA3<br>... |
| Server | Server 1 IP←→ IGA1<br>Server 2 IP←→ IGA1<br>Server 3 IP←→ IGA1 |

## 8.6.6 Port Translation

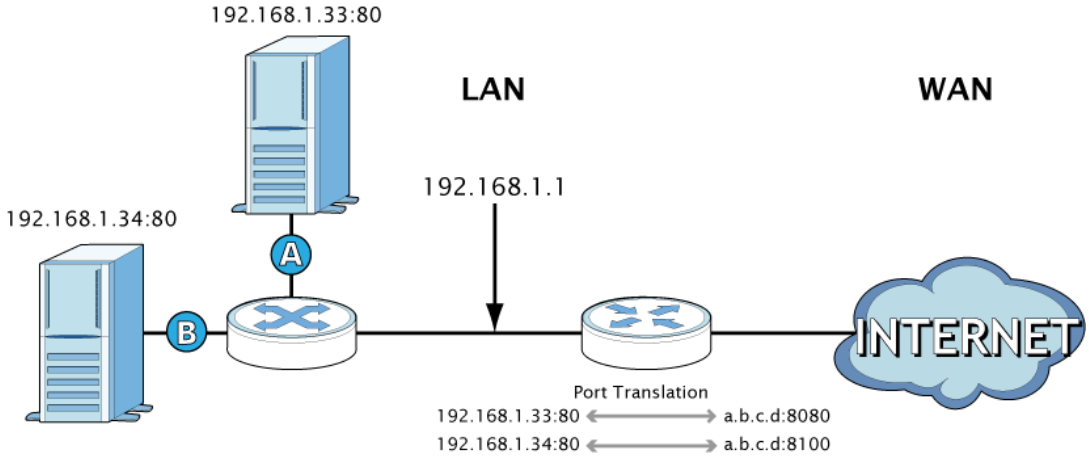
The P-660H-T1v3s can translate the destination port number or a range of port numbers of packets coming from the WAN to another destination port number or range of port numbers on the local network. When you use port forwarding without port translation, a single server on the local network can use a specific port number and be accessible to the outside world through a single WAN IP address. When you use port translation with port forwarding, multiple servers on the local network can use the same port number and still be accessible to the outside world through a single WAN IP address.

The following example has two web servers on a LAN. Server **A** uses IP address 192.168.1.33 and server **B** uses 192.168.1.34. Both servers use port 80. The letters a.b.c.d represent the WAN port's IP address. The P-660H-T1v3s translates port 8080 of traffic received on the WAN port (IP address a.b.c.d) to port 80 and sends it to server **A** (IP address 192.168.1.33). The P-660H-T1v3s also translates

port 8100 of traffic received on the WAN port (also IP address a.b.c.d) to port 80, but sends it to server **B** (IP address 192.168.1.34).

Note: In this example, anyone wanting to access server A from the Internet must use port 8080. Anyone wanting to access server B from the Internet must use port 8100.

**Figure 45** Port Translation Example



# 9

# Firewalls

## 9.1 Overview

This chapter shows you how to enable the P-660H-T1v3s firewall. Use the firewall to protect your P-660H-T1v3s and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.
- blocks SYN and port scanner attacks.

By default, the P-660H-T1v3s blocks DDOS, LAND and Ping of Death attacks whether the firewall is enabled or disabled.

### 9.1.1 What You Can Do in the Firewall Screens

Use the **Firewall** screen (Section 9.2 on page 123) to enable firewall and/or SPI on the P-660H-T1v3s.

### 9.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

#### SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

### DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

### DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

### LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

### Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

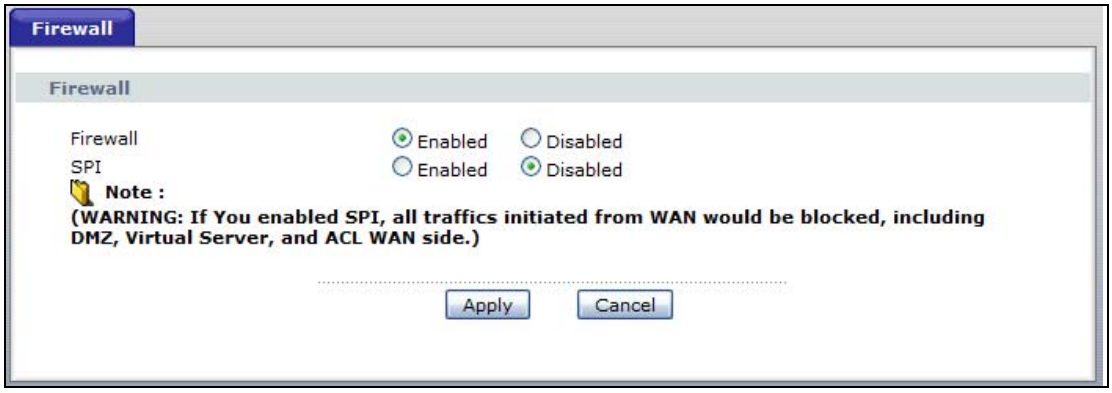
### SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

# 9.2 The Firewall Screen

Use this screen to enable firewall and/or SPI. Click **Advanced Setup > Firewall** to display the following screen.

**Figure 46** Advanced Setup > Firewall




The following table describes the labels in this screen.

**Table 30** Advanced > Firewall

| LABEL | DESCRIPTION |
|---|---|
| Firewall | Use this field to enable or disable firewall on your P-660H-T1v3s. |
| SPI | Use this field to enable or disable SPI on your P-660H-T1v3s. |
| SAVE | Click this to save your changes. |
| CANCEL | Click this to restore your previously saved settings. |

**Enabling SPI blocks all traffic initiated from the WAN side, including the DMZ, virtual server and ACL on the WAN side.**

# 10 Filters

## 10.1 Overview

This chapter introduces three types of filters supported by the P-660H-T1v3s. You can configure rules to restrict traffic by IP addresses, MAC addresses, application types and/or URLs.

### 10.1.1 What You Can Do in the Filter Screens

- Use the **URL Filter** screen (Section 10.2 on page 126) to block access to web sites.
- Use the **Application Filter** screen (Section 10.3 on page 127) to allow or deny traffic from certain types of applications.
- Use the **IP/MAC Filter** screen (Section 10.4 on page 128) to create IP/MAC filter rules.

### 10.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

#### IP/MAC Filter Structure

An IP/MAC filter set consists of one or more filter rules. The P-660H-T1v3s allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

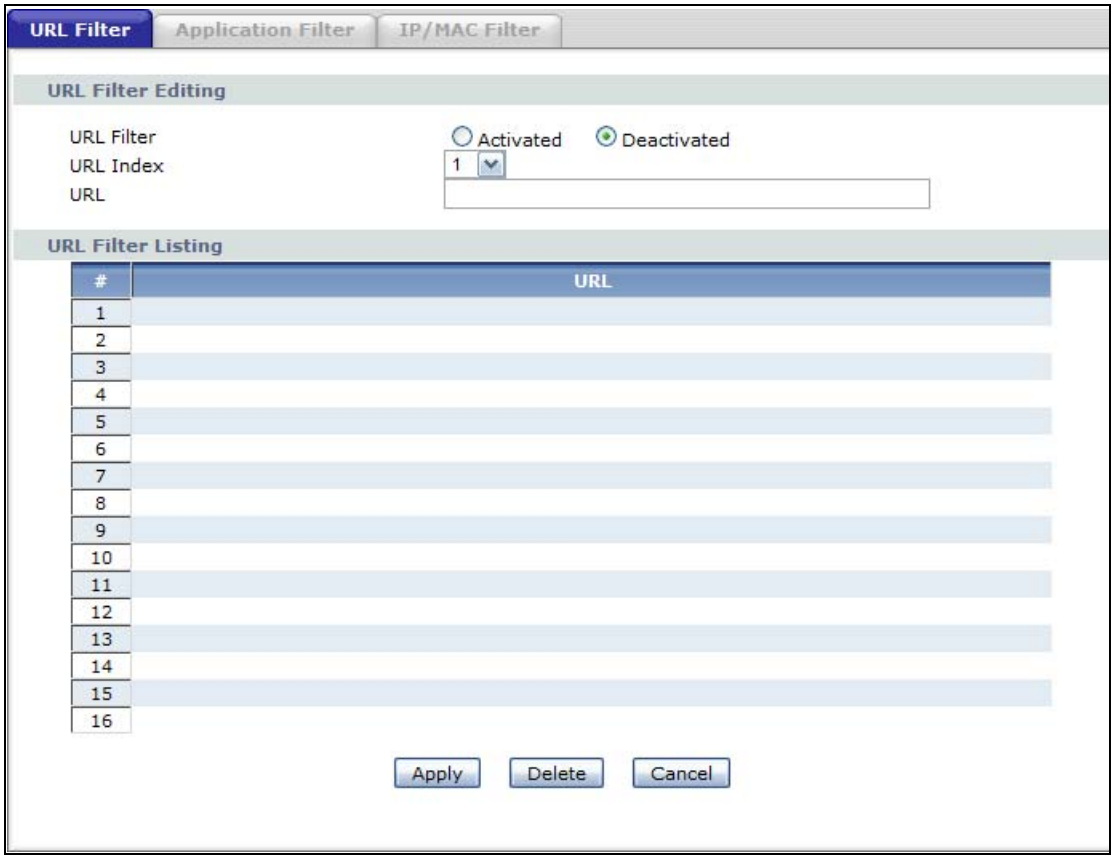
#### URL

The URL (Uniform Resource Locator) identifies and helps locates resources on a network. On the Internet the URL is the web address that you type in the address bar of your Internet browser, for example “http://www.zyxel.com”.

# 10.2 The URL Filter Screen

Use this screen to block websites by URL. Click **Security** > **Filter** and select **URL Filter** in the **Filter Type Selection** field.. The screen appears as shown.

**Figure 47** Security > Filter > URL Filter




The following table describes the labels in this screen.

**Table 31** Security > Filter > URL Filter

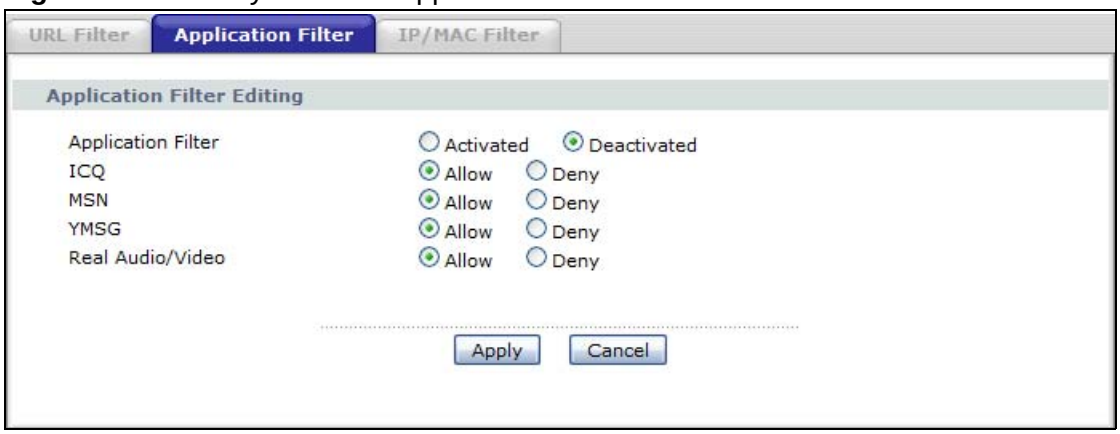
| LABEL | DESCRIPTION |
|---|---|
| URL Filter Editing | |
| Active | Use this field to enable or disable the URL filter. |
| URL Index | Select the index number of the filter. |
| URL | Enter the URL for the P-660H-T1v3s to block. |
| URL Filter Listing | |
| Index | This is the index number of the filter rule. |
| URL | This is the URL you have configured the P-660H-T1v3s to block. |
| Apply | Click this to save your changes. |
| Delete | Click this to remove the filter rule. |
| Cancel | Click this to restore your previously saved settings. |

# 10.3 The Application Filter Screen

Use this screen to allow or deny traffic for certain types of applications. The application filter provides a convenient way to manage the use of various applications on the network.

Click **Security** > **Filter** and select **Application Filter** in the **Filter Type Selection** field. The screen appears as shown.

**Figure 48** Security > Filter > Application Filter




The following table describes the labels in this screen.

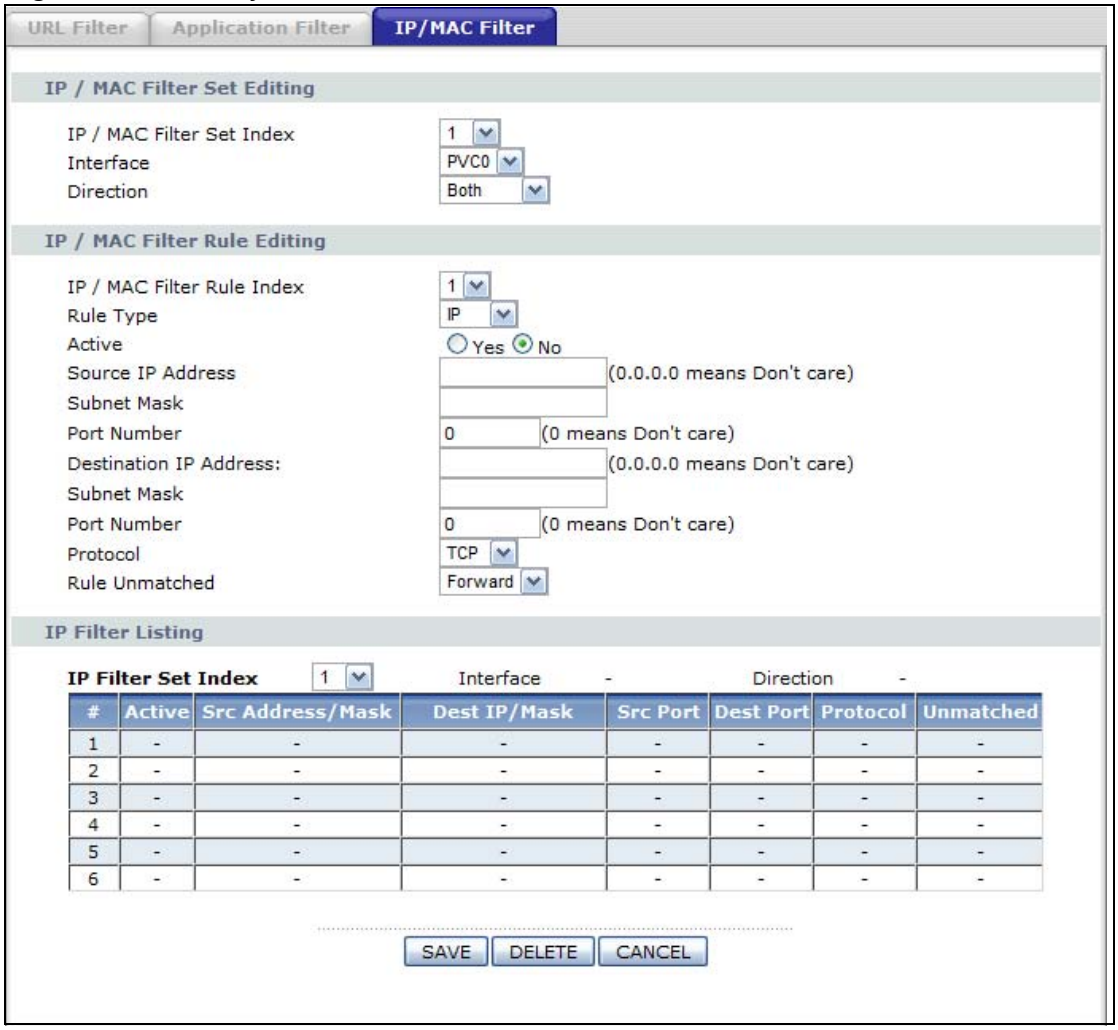
**Table 32** Security > Filter > Application Filter

| LABEL | DESCRIPTION |
|---|---|
| Application Filter | Use this field to enable or disable the application filter. |
| ICQ | Use this field to allow or deny ICQ traffic. |
| MSN | Use this field to allow or deny MSN traffic. |
| YMSG | Use this field to allow or deny Yahoo Messenger traffic |
| Real Audio/Video | Use this field to allow or deny transferring RealPlayer format files. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 10.4 The IP/MAC Filter Screen

Use this screen to create and apply IP/MAC filters. Click **Security** > **Filter** and select **IP/MAC Filter** in the **Filter Type Selection** field. The screen appears as shown.

**Figure 49** Security> Filter / IP/MAC Filter




The following table describes the labels in this screen.

**Table 33** Security > Filter > IP/MAC Filter

| LABEL | DESCRIPTION |
|---|---|
| IP/MAC Filter Set Editing | |
| IP/MAC Filter Set Index | Select the index number of the filter set. |
| Interface | Select the PVC to which to apply the filter. |
| Direction | Apply the filter to **Both**, **Incoming** or **Outgoing** traffic direction. |
| IP/MAC Filter Rule Editing | |

**Table 33** Security > Filter > IP/MAC Filter (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP/MAC Filter Rule Index | Select the index number of the filter rule. |
| Rule Type | Select **IP** or **MAC** type to configure the rule.<br>Use the **IP Filter** to block traffic by IP addresses.<br>Use the **MAC Filter** to block traffic by MAC address. |
| Active | Use this field to enable or disable the rule. |
| Source IP Address | Enter the source IP address of the packets you wish to filter. This field is ignored if it is 0.0.0.0. |
| Subnet Mask | Enter the IP subnet mask for the source IP address |
| Port Number | Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0. |
| Destination IP Address | Enter the destination IP address of the packets you wish to filter. This field is ignored if it is 0.0.0.0. |
| Subnet Mask | Enter the IP subnet mask for the destination IP address. |
| Port Number | Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0. |
| Protocol | Select **ICMP**, **TCP** or **UDP** for the upper layer protocol. |
| MAC Address | This field is only available when you select **MAC** in the **Rule Type** field.<br>Enter the MAC address of the packets you wish to filter. |
| Rule Unmatched | Select the action for a packet not matching the rule.<br>Select **Forward** to forward traffic immediately and skip checking the remaining rules. Select **Next** to check the next rule. |
| IP/MAC Filter Listing | |
| IP/MAC Filter Set Index | Select the index number of the filter set from the drop-downl list box. |
| Interface | This is the interface that the filter set applies to. |
| Direction | The filter set applies to this traffic direction. |
| # | This is the index number of the rule in a filter set. |
| Active | This field shows whether the rule is activated. |
| Src Address/Mask | This is the source IP address and subnet mask when you select **IP** as the rule type.<br>This is the MAC address when you select **MAC** as the rule type. |
| Dest IP/Mask | This is the destination IP address and subnet mask. |
| Src Port | This is the source port number. |
| Dest Port | This is the destination port number. |
| Protocol | This is the upper layer protocol. |
| Unmatched | When a packet doesn't match the rule, this is the action the P-660H-T1v3s takes on the packet. |

**Table 33** Security > Filter > IP/MAC Filter (continued)

| LABEL | DESCRIPTION |
|---|---|
| SAVE | Click this to save your changes. |
| DELETE | Click this to remove the filter rule. |
| CANCEL | Click this to restore your previously saved settings. |

# 11

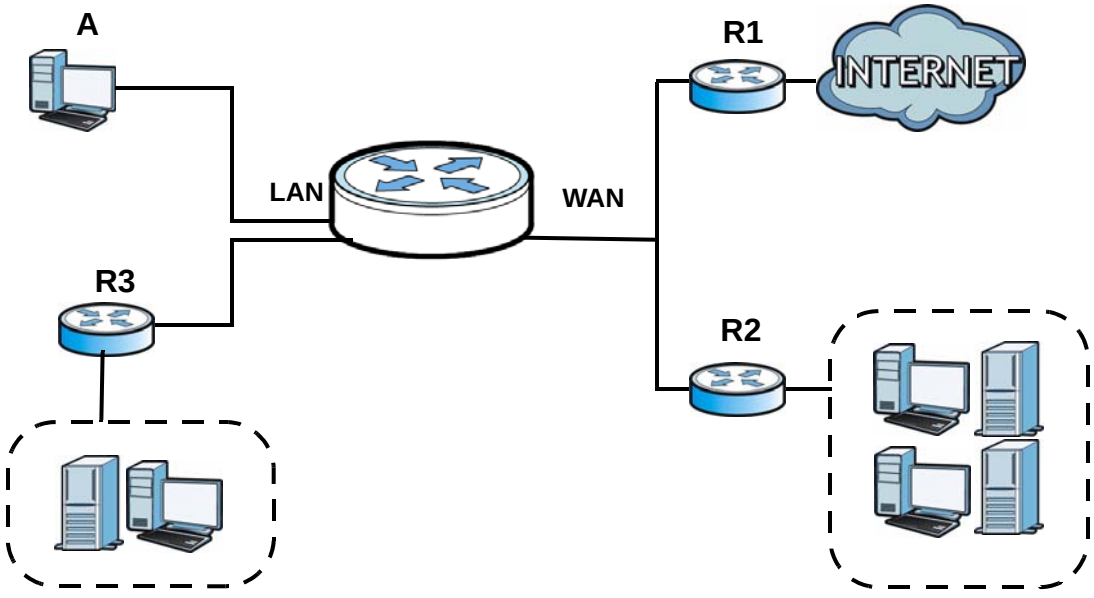
# Static Route

## 11.1 Overview

The P-660H-T1v3s usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the P-660H-T1v3s send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the P-660H-T1v3s's LAN interface. The P-660H-T1v3s routes most traffic from **A** to the Internet through the P-660H-T1v3s's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

**Figure 50** Example of Static Routing Topology



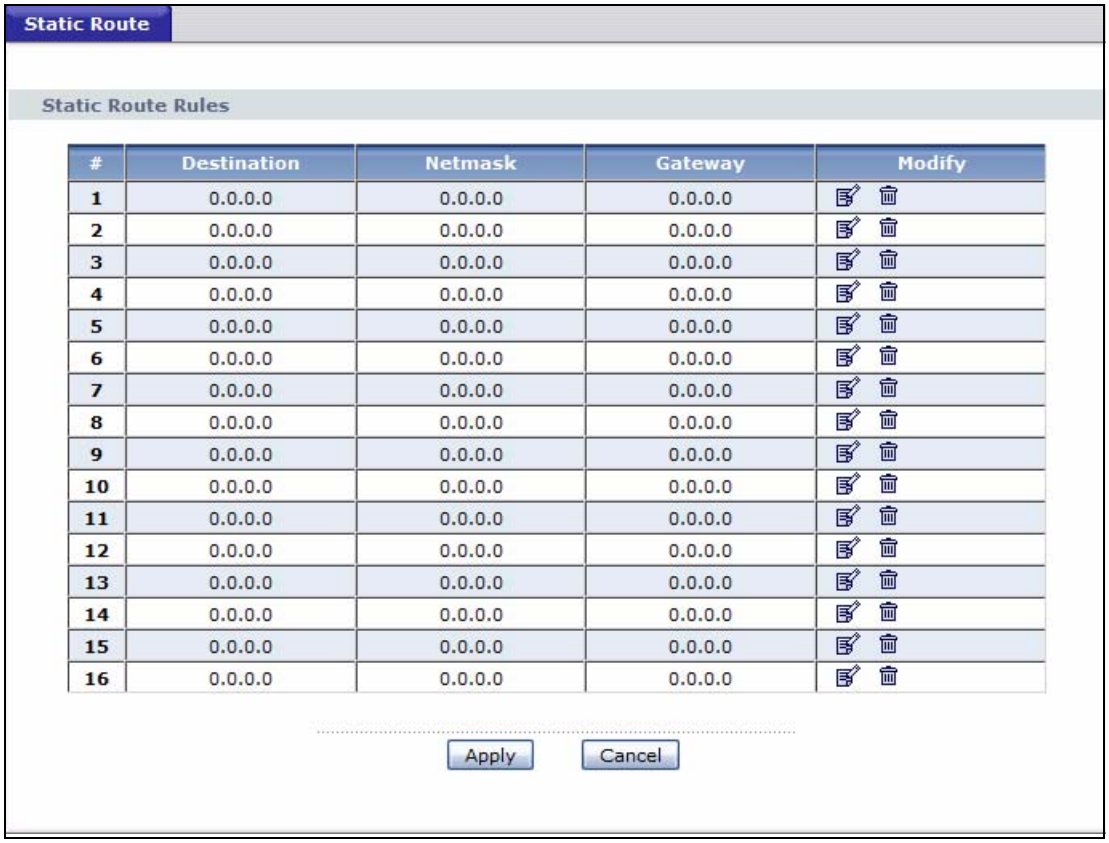

### 11.1.1 What You Can Do in the Static Route Screens

Use the **Static Route** screens (Section 11.2 on page 132) to view and configure IP static routes on the P-660H-T1v3s.

# 11.2 The Static Route Screen

Use this screen to view the static route rules. Click **Advanced > Static Route** to open the **Static Route** screen.

**Figure 51** Advanced > Static Route




The following table describes the labels in this screen.

**Table 34** Advanced > Static Route

| LABEL | DESCRIPTION |
|---|---|
| Destination | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| Netmask | This parameter specifies the IP network subnet mask of the final destination. |
| Gateway | This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Modify | Click the **Edit** icon to go to the screen where you can set up a static route on the P-660H-T1v3s.<br><br>Click the **Remove** icon to remove a static route from the P-660H-T1v3s. A window displays asking you to confirm that you want to delete the route. |

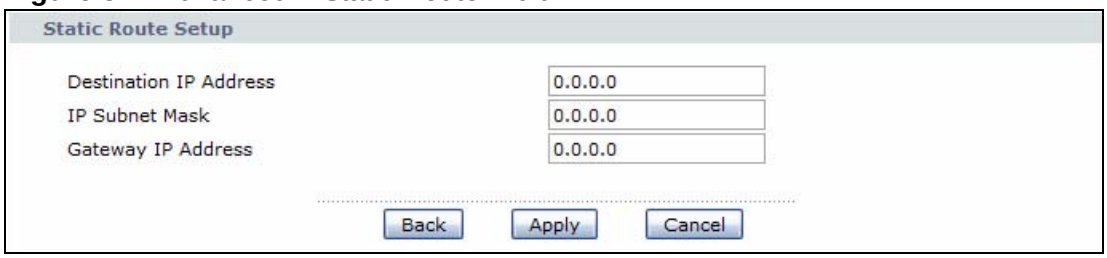
**Table 34** Advanced > Static Route

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

## 11.2.1 Static Route Edit

Use this screen to configure the required information for a static route. Select a static route index number and click **Edit**. The screen shown next appears.

**Figure 52** Advanced > Static Route: Edit




The following table describes the labels in this screen.

**Table 35** Advanced > Static Route: Edit

| LABEL | DESCRIPTION |
|---|---|
| Destination IP Address | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |
| IP Subnet Mask | Enter the IP subnet mask here. |
| Gateway Type | Use either **Gateway Address** or **Gateway Node** to configure a static route. |
| Gateway IP Address | This field is available when you select **Gateway Address** from **Gateway Type**.<br><br>Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Back | Click this to return to the previous screen without saving. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 12

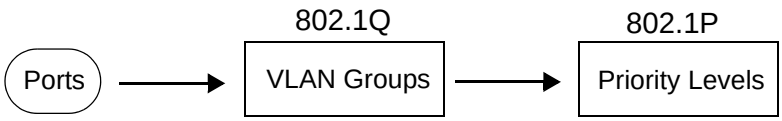
# 802.1Q/1P

## 12.1 Overview

This chapter describes how to configure the 802.1Q/1P settings.

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. A VLAN group can be treated as an individual device. Each group can have its own rules about where and how to forward traffic. You can assign any ports on the P-660H-T1v3s to a VLAN group and configure the settings for the group. You may also set the priority level for traffic trasmitted through the ports.

**Figure 53** 802.1Q/1P




### 12.1.1 What You Can Do in the 802.1Q/1P Screens

- Use the **Group Setting** screen (Section 12.2 on page 137) to activate 802.1Q/1P, specify the management VLAN group, display the VLAN groups and configure the settings for each VLAN group.
- Use the **Port Setting** screen (Section 12.3 on page 140) to configure the PVID and assign traffic priority for each port.

### 12.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

#### IEEE 802.1P Priority

IEEE 802.1P specifies the user priority field and defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.

### IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the device on which they were created. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

### PVC

A virtual circuit is a logical point-to-point circuit between customer sites. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.

### Forwarding Tagged and Untagged Frames

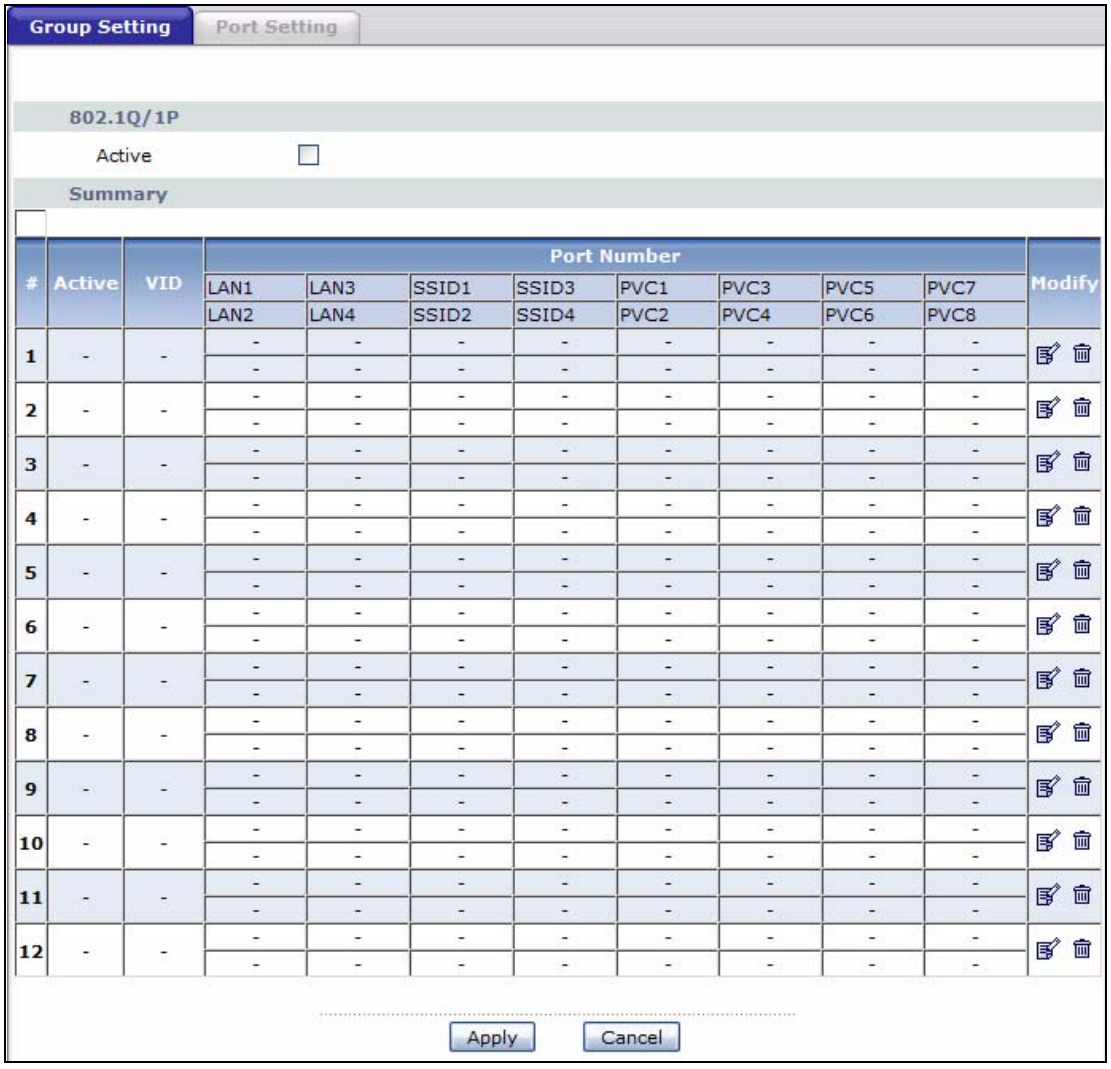
Each port on the device is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware device to an 802.1Q VLAN-unaware device, the P-660H-T1v3s first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware device to an 802.1Q VLAN-aware switch, the P-660H-T1v3s first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

Whether to tag an outgoing frame depends on the setting of the egress port on a per-VLAN, per-port basis (recall that a port can belong to multiple VLANs). If the tagging on the egress port is enabled for the VID of a frame, then the frame is transmitted as a tagged frame; otherwise, it is transmitted as an untagged frame.

# 12.2 The Group Setting Screen

Use this screen to activate 802.1Q/1P and display the VLAN groups. Click **Advanced > 802.1Q/1P** to display the following screen.

**Figure 54** Advanced > 802.1Q/1P > Group Setting




The following table describes the labels in this screen.

**Table 36** Advanced > 802.1Q/1P > Group Setting

| LABEL | DESCRIPTION |
|---|---|
| 802.1Q/1P | |
| Active | Select this check box to activate the 802.1P/1Q feature. |
| Summary | |
| # | This field displays the index number of the VLAN group. |
| Active | This field indicates whether the VLAN group is active or not. |
| VID | This field displays the ID number of the VLAN group. |

**Table 36** Advanced > 802.1Q/1P > Group Setting (continued)

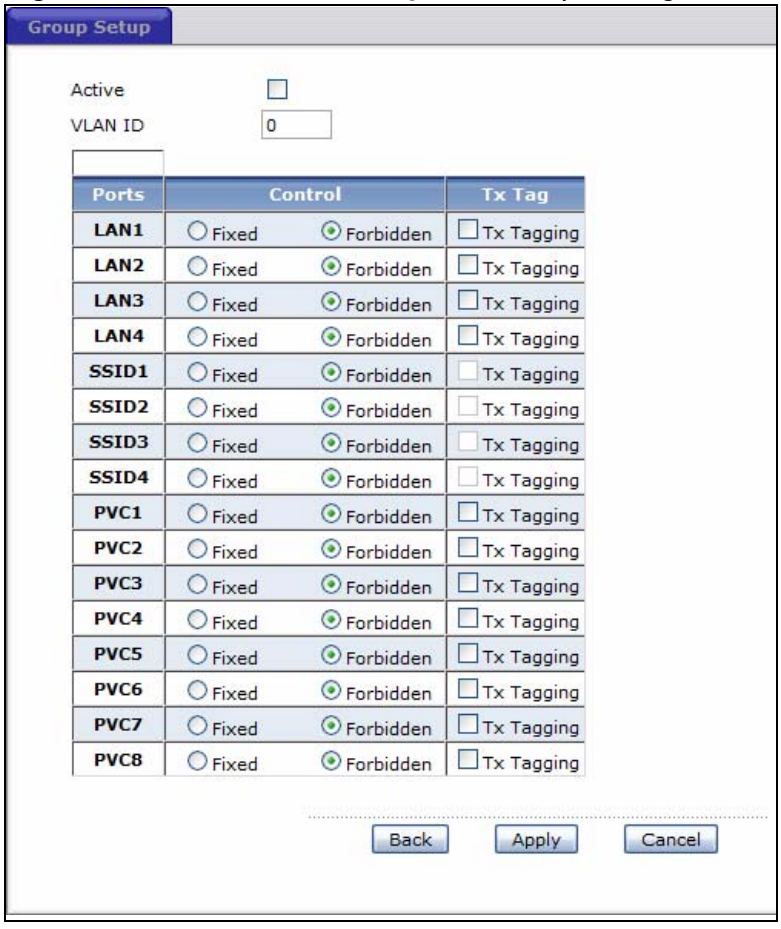
| LABEL | DESCRIPTION |
|---|---|
| Port Number | These columns display the VLAN's settings for each port. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**". |
| Modify | Click the **Edit** button to configure the the ports in the VLAN group.<br>Click the **Remove** button to delete the VLAN group. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

## 12.2.1 Editing 802.1Q/1P Group Setting

Use this screen to configure the settings for each VLAN group.

In the **802.1Q/1P** screen, click the **Edit** button from the **Modify** filed to display the following screen.

**Figure 55** Advanced > 802.1Q/1P > Group Setting > Edit



The following table describes the labels in this screen.

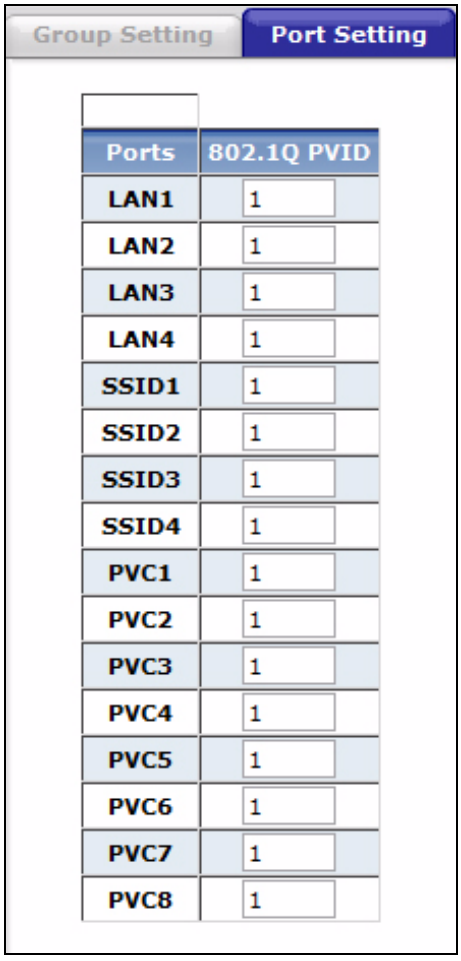
**Table 37** Advanced > 802.1Q/1P > Group Setting > Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this to make this VLAN group active. |
| VLAN ID | Assign a VLAN ID for the VLAN group. The valid VID range is between 1 and 4094. |
| Ports | This field displays the types of ports available to join the VLAN group. |
| Control | Select **Fixed** for the port to be a permanent member of the VLAN group.<br>Select **Forbidden** if you want to prohibit the port from joining the VLAN group. |
| Tx Tag | Select **Tx Tagging** if you want the port to tag all outgoing traffic trasmitted through this VLAN. You select this if you want to create VLANs across different devices and not just the P-660H-T1v3s. |
| Back | Click this to return to the previous screen without saving. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 12.3 The 802.1Q/1P Port Setting Screen

Use this screen to configure the PVID and assign traffic priority for each port. Click **Advanced** > **802.1Q/1P** > **Port Setting** to display the following screen.

**Figure 56** Advanced > 802.1Q/1P > Port Setting




The following table describes the labels in this screen.

**Table 38** Advanced > 802.1Q/1P > Port Setting

| LABEL | DESCRIPTION |
|---|---|
| Ports | This field displays the types of ports available to join the VLAN group. |
| 802.1Q PVID | Assign a VLAN ID for the port. The valid VID range is between 1 and 4094. The P-660H-T1v3s assigns the PVID to untagged frames or priority-tagged frames received on this port. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 13

# Quality of Service (QoS)

## 13.1 Overview

Use the **QoS** screen to set up your P-660H-T1v3s to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control bandwidth. QoS allows the P-660H-T1v3s to group and prioritize application traffic and fine-tune network performance.

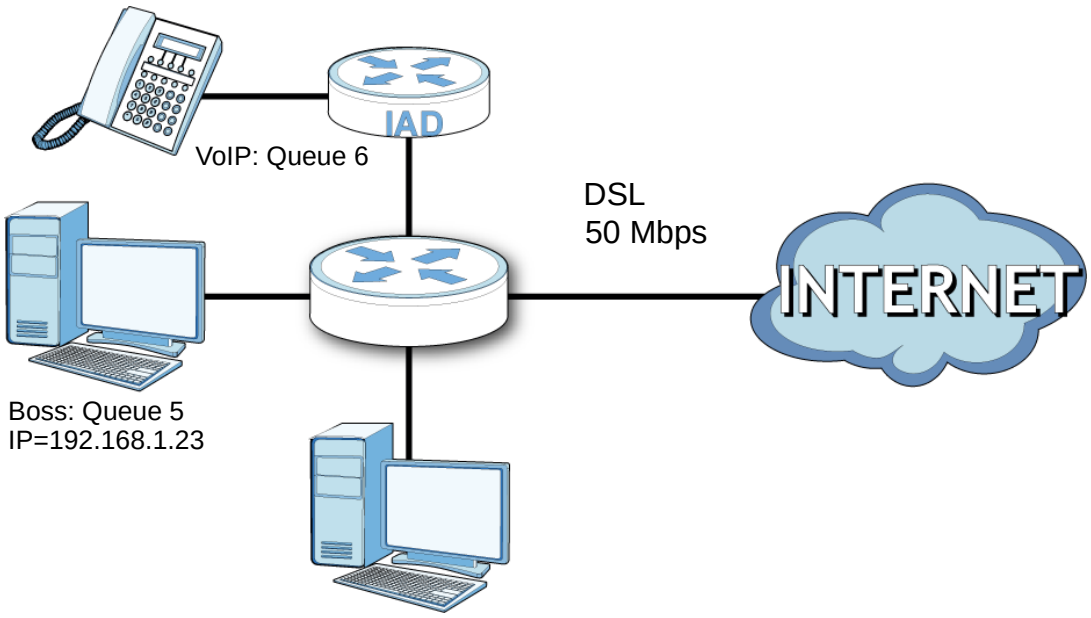
Without QoS, all traffic data are equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

The P-660H-T1v3s assigns each packet a priority and then queues the packet accordingly. Packets assigned with a high priority are processed more quickly than those with low priorities if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

In the following figure, your Internet connection has an upstream transmission speed of 50 Mbps. You configure a classifier to assign the highest priority queue (6) to VoIP traffic from the LAN interface, so that voice traffic would not get delayed when there is network congestion. Traffic from the boss's IP address (192.168.1.23 for example) is mapped to queue 5. Traffic that does not match

these two classes are assigned priority queue based on the internal QoS mapping table on the P-660H-T1v3s.

**Figure 57** QoS Example




## 13.1.1 What You Can Do in the QoS Screens

- Use the **QoS** screen (Section 13.2 on page 143) to configure QoS settings on the P-660H-T1v3s.
- Use the **QoS Settings Summary** screen (Section 13.2.1 on page 145) to check the summary of QoS rules and actions you configured for the P-660H-T1v3s.

## 13.1.2 What You Need to Know

The following terms and concepts may help as you read through the chapter.

### 802.1p

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. 802.1p is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use 802.1p to give different priorities to different packet types.

### Tagging and Marking

In a QoS class, you can configure whether to add or change the DiffServ Code Point (DSCP) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking

device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

### Finding Out More

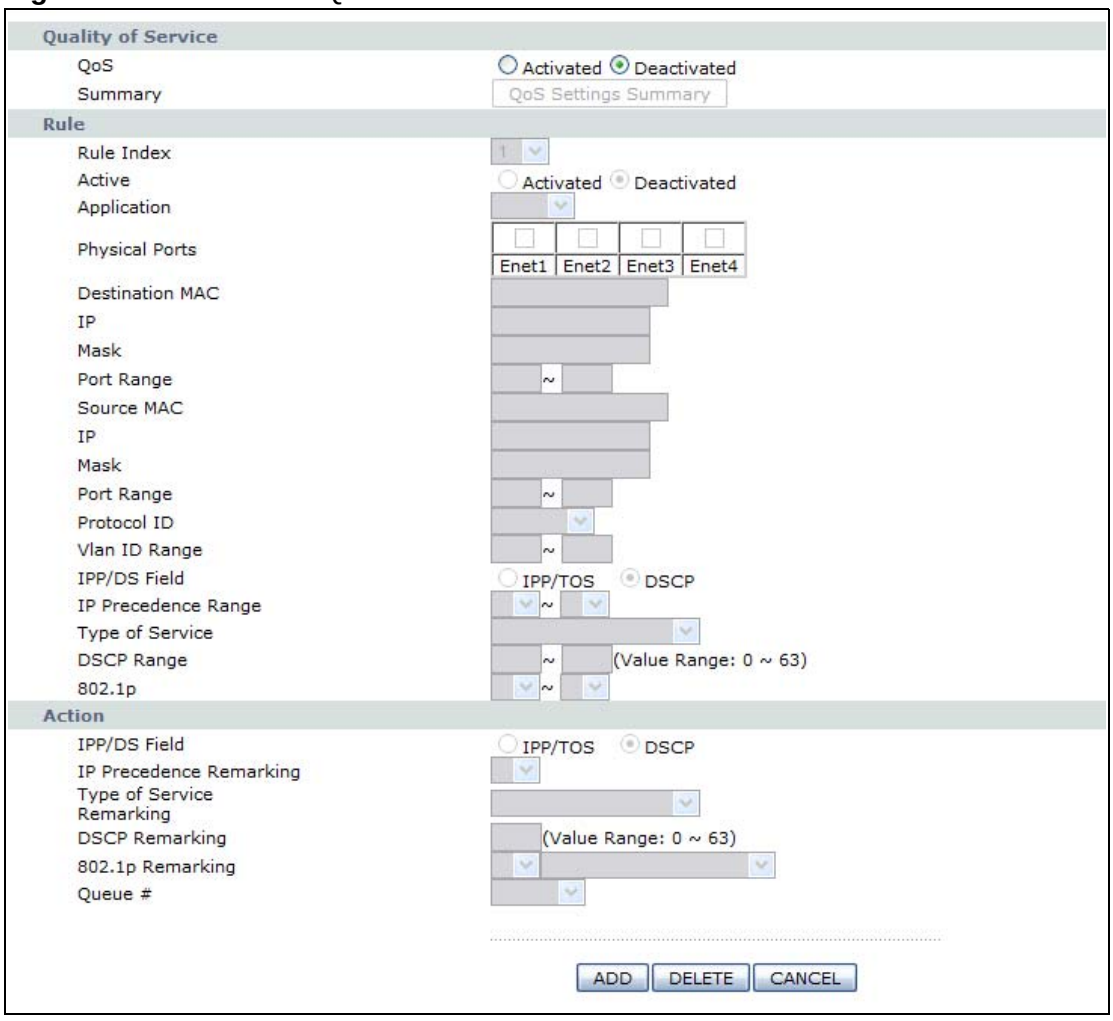
See Section 13.3 on page 146 for advanced technical information on QoS.

## 13.2 The QoS Screen

Use this screen to enable or disable QoS and have the P-660H-T1v3s assign priority levels to traffic according to the port range, IEEE 802.1p priority level and/or IP precedence.

Click **Advanced Setup > QoS** to open the screen as shown next.

**Figure 58** Advanced > QoS



The following table describes the labels in this screen.

**Table 39** Advanced > QoS

| LABEL | DESCRIPTION |
|---|---|
| Quality of Service | |
| QoS | Use this field to turn on QoS to improve your network performance.<br><br>You can give priority to traffic that the P-660H-T1v3s forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications. |
| Summary | Click this to open a summary table showing the QoS settings. |
| Rule | |
| Rule Index | Select the rule's index number from the drop-down list box. |
| Active | Use this field to enable or disable the rule. |
| Application | Select an application from the drop-down list box. The **Destination Port Range** and **Protocol ID** fields may change depending on the type of applications you choose. |
| Physical Ports | Select an Ethernet port to which to apply the rule. |
| Destination MAC | Type a destination MAC address here. QoS is then applied to traffic containing this destination MAC address. Leave it blank to apply the rule to all MAC addresses. |
| IP | Enter a destination IP address in dotted decimal notation. QoS is then applied to traffic containing this destination IP address. A blank destination IP address means any destination IP address. |
| Mask | Enter a destination subnet mask here. |
| Port Range | Either use the default value set by the application you choose, or enter the port number to which the rule should be applied. |
| Source MAC | Type a source MAC address here. QoS is then applied to traffic containing this source MAC address. Leave it blank to apply the rule to all MAC addresses. |
| IP | Enter a source IP address in dotted decimal notation. QoS is then applied to traffic containing this source IP address. A blank source IP address means any source IP address. |
| Mask | Enter a source subnet mask here. |
| Port Range | Enter the port number to which the rule should be applied. 0 means any source port number. |
| Protocol ID | Select an IP protocol type from the drop-down list box. |
| Vlan ID Range | Enter the source VLAN ID in this field. |
| IPP/DS Field | Select **IPP/TOS** to specify an IP precedence range and type of services.<br><br>Select **DSCP** to specify a DiffServ Code Point (DSCP) range. |
| IP Precedence Range | Enter a range from 0 to 7 for IP precedence. Zero is the lowest priority and seven is the highest. |
| Type of Service | Select a type of service from the drop-down list box.<br><br>Available options are: **Normal service**, **Minimize delay**, **Maximize throughput**, **Maximize reliability** and **Minimize monetary cost**. |
| DSCP Range | Specify a DSCP number between 0 and 63 in this field. |

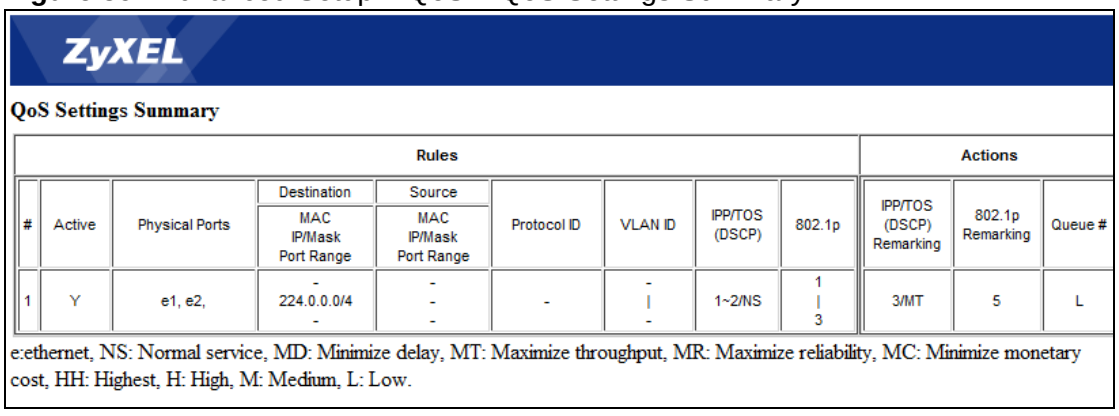
**Table 39** Advanced > QoS

| LABEL | DESCRIPTION |
|---|---|
| 802.1p | Select a priority level (0 to 7) from the drop-down list box. |
| Action | |
| IPP/DS Field | Select **IPP/TOS** to specify an IP precedence range and type of services.<br>Select **DSCP** to specify a DiffServ Code Point (DSCP) range. |
| IP Precedence Remarking | Enter a range from 0 to 7 to re-assign IP precedence to matched traffic. Zero is the lowest priority and seven is the highest. |
| Type of Service Remarking | Select a type of service to re-assign the priority level to matched traffic.<br>Available options are: **Normal service**, **Minimize delay**, **Maximize throughput**, **Maximize reliability** and **Minimize monetary cost**. |
| DSCP Remarking | Specify a DSCP number between 0 and 63 to re-assign the priority level to matched traffic. |
| 802.1p Remarking | Select a priority level (0 to 7) to re-assign the priority level to matched traffic. |
| Queue # | Specify a **Low**, **Medium**, **High** or **Highest** queue tag to matched traffic. Traffic assigned to a higher queue gets through faster while traffic in lower queues is dropped when there is network congestion. |
| ADD | Click this to add the rule. |
| DELETE | Click this to remove the rule. |
| CANCEL | Click this to restore previously saved settings. |

## 13.2.1 The QoS Settings Summary Screen

Use this screen to display a summary of rules and actions configured for the P-660H-T1v3s. In the **Advanced > QoS** screen, click the **QoS Settings Summary** button to open the following screen.

**Figure 59** Advanced Setup > QoS > QoS Settings Summary


ZyXEL
QoS Settings Summary
Rules
Actions
# Active Physical Ports Destination MAC IP/Mask Port Range Source MAC IP/Mask Port Range Protocol ID VLAN ID IPP/TOS (DSCP) 802.1p IPP/TOS (DSCP) Remarking 802.1p Remarking Queue #
1 Y e1, e2, - 224.0.0.0/4 - - - - - - - 1~2/NS 1 | 3 3/MT 5 L
e:ethernet, NS: Normal service, MD: Minimize delay, MT: Maximize throughput, MR: Maximize reliability, MC: Minimize monetary cost, HH: Highest, H: High, M: Medium, L: Low.

The following table describes the labels in this screen.

**Table 40** Advanced Setup > QoS > QoS Settings Summary

| LABEL | DESCRIPTION |
|---|---|
| Rules | |
| # | This is the rule's index number. |
| Active | This shows whether the rule is enabled or disabled. |
| Physical Ports | This is the physical port associated with the rule. |
| Destination MAC and IP/Mask Port Ranges | This is the port range for destination MAC address and IP address. |
| Source MAC and IP/Mask Port Ranges | This is the port range for source MAC address and IP address. |
| Protocol ID | This is the protocol ID associated with the rule. |
| VLAN ID | This is the VLAN ID associated with the rule. |
| IPP/TOS (DSCP) | This shows the IPP/TOS or DSCP settings. |
| 802.1p | This is the 802.1p priority level. |
| Actions | |
| IPP/TOS (DSCP) Remarking | The P-660H-T1v3s re-assigns the priority values specified in this field to matched traffic. |
| 802.1p Remarking | The P-660H-T1v3s re-assigns the priority levels specified in this field to matched traffic. |
| Queue # | The P-660H-T1v3s assigns the queue level specified in this field to matched traffic. |

# 13.3 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

## 13.3.1 IEEE 802.1p

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

**Table 41** IEEE 802.1p Priority Level and Traffic Type

| PRIORITY LEVEL | TRAFFIC TYPE |
|---|---|
| Level 7 | Typically used for network control traffic such as router configuration messages. |
| Level 6 | Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay). |

**Table 41** IEEE 802.1p Priority Level and Traffic Type

| PRIORITY LEVEL | TRAFFIC TYPE |
|---|---|
| Level 5 | Typically used for video that consumes high bandwidth and is sensitive to jitter. |
| Level 4 | Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions. |
| Level 3 | Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay. |
| Level 2 | This is for “spare bandwidth”. |
| Level 1 | This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users. |
| Level 0 | Typically used for best-effort traffic. |

## 13.3.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

## 13.3.3 Automatic Priority Queue Assignment

If you enable QoS on the P-660H-T1v3s, the P-660H-T1v3s can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the P-660H-T1v3s. On the P-660H-T1v3s, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

**Table 42** Internal Layer2 and Layer3 QoS Mapping

| PRIORITY QUEUE | LAYER 2 | LAYER 3 | | |
|---|---|---|---|---|
| | IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY) | TOS (IP PRECEDENCE) | DSCP | IP PACKET LENGTH (BYTE) |
| 0 | 1 | 0 | 000000 | |
| 1 | 2 | | | |
| 2 | 0 | 0 | 000000 | >1100 |

**Table 42** Internal Layer2 and Layer3 QoS Mapping

| PRIORITY QUEUE | LAYER 2 | LAYER 3 | | |
|---|---|---|---|---|
| | IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY) | TOS (IP PRECEDENCE) | DSCP | IP PACKET LENGTH (BYTE) |
| 3 | 3 | 1 | 001110<br>001100<br>001010<br>001000 | 250~1100 |
| 4 | 4 | 2 | 010110<br>010100<br>010010<br>010000 | |
| 5 | 5 | 3 | 011110<br>011100<br>011010<br>011000 | <250 |
| 6 | 6 | 4 | 100110<br>100100<br>100010<br>100000 | |
| | | 5 | 101110<br>101000 | |
| 7 | 7 | 6 | 110000 | |
| | | 7 | 111000 | |

# 14

# Dynamic DNS Setup

## 14.1 Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

### 14.1.1 What You Can Do in the DDNS Screen

Use the **Dynamic DNS** screen (Section 14.2 on page 150) to enable DDNS and configure the DDNS settings on the P-660H-T1v3s.

### 14.1.2 What You Need To Know About DDNS

#### DYNDNS Wildcard

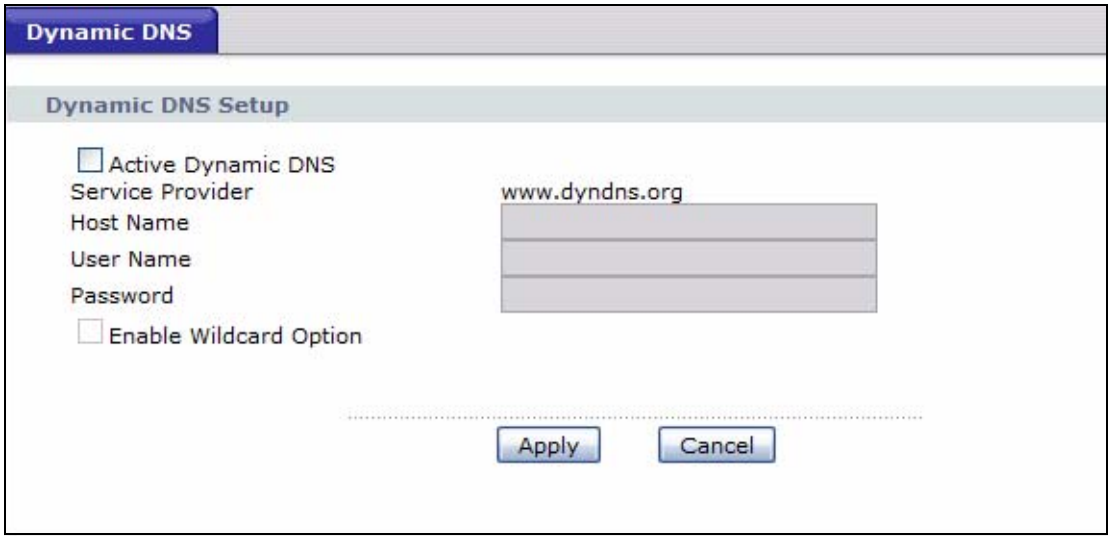
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

# 14.2 The Dynamic DNS Screen

Use this screen to change your P-660H-T1v3s's DDNS. Click **Advanced > Dynamic DNS**. The screen appears as shown.

**Figure 60** Advanced > Dynamic DNS




The following table describes the fields in this screen.

**Table 43** Advanced > Dynamic DNS

| LABEL | DESCRIPTION |
|---|---|
| Dynamic DNS Setup | |
| Active Dynamic DNS | Select this check box to use dynamic DNS. |
| Service Provider | This is the name of your Dynamic DNS service provider. |
| Dynamic DNS Type | Select the type of service that you are registered for from your Dynamic DNS service provider. |
| Host Name | Type the domain name assigned to your P-660H-T1v3s by your Dynamic DNS provider.<br>You can specify up to two host names in the field separated by a comma (","). |
| User Name | Type your user name. |
| Password | Type the password assigned to you. |
| Enable Wildcard Option | Select the check box to enable DynDNS Wildcard. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 15

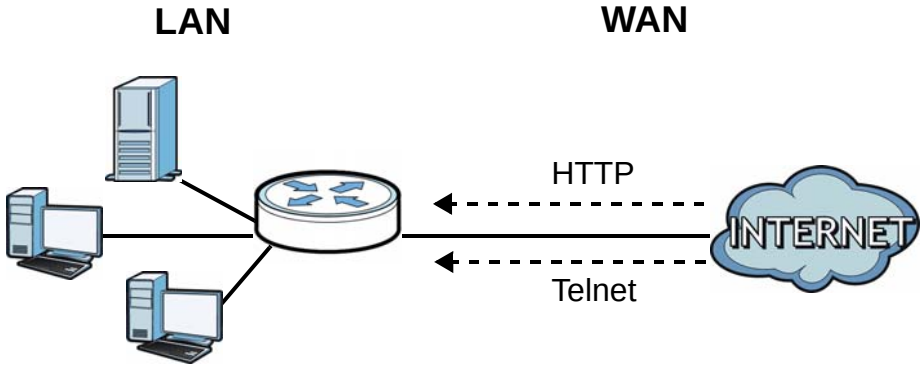
# Remote Management

## 15.1 Overview

Remote management allows you to determine which services/protocols can access which P-660H-T1v3s interface (if any) from which computers.

The following figure shows remote management of the P-660H-T1v3s coming in from the WAN.

**Figure 61** Remote Management From the WAN




Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

You may manage your P-660H-T1v3s from a remote location via:

- Internet (WAN only)
- LAN only
- WLAN only
- LAN and WAN
- LAN and WLAN
- WLAN and WAN
- ALL (WAN, LAN and WLAN)
- None (Disable)

To disable remote management of a service, select **Disable** in the corresponding **Access Status** field.

You may only have one remote management session running at a time. The P-660H-T1v3s automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1 Telnet

2 HTTP

## 15.1.1 What You Can Do in the Remote Management Screens

- Use the **WWW** screen (Section 15.2 on page 153) to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the P-660H-T1v3s.
- Use the **Telnet** screen (Section 15.3 on page 154) to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the P-660H-T1v3s.
- Use the **FTP** screen (Section 15.4 on page 155) to configure through which interface(s) and from which IP address(es) users can use FTP to access the P-660H-T1v3s.
- Use the **SNMP** screen (Section 15.5 on page 156) toto set up SNMP access for your P-660H-T1v3s.
- Use the **DNS** screen (Section 15.6 on page 157) to configure through which interface(s) and from which IP address(es) users can send DNS queries to the P-660H-T1v3s.
- Use the **ICMP** screen (Section 15.7 on page 158) to set whether or not your P-660H-T1v3s will respond to pings and probes for services that you have not made available.

## 15.1.2 What You Need to Know

The following terms and concepts may help as you read the chapter.

### Remote Management Limitations

Remote management does not work when:

- You have not enabled that service on the interface in the corresponding remote management screen.
- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the P-660H-T1v3s will disconnect the session immediately.

- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- There is a firewall rule that blocks it.

### Remote Management and NAT

When NAT is enabled:

- Use the P-660H-T1v3s's WAN IP address when configuring from the WAN.
- Use the P-660H-T1v3s's LAN IP address when configuring from the LAN.

### System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The P-660H-T1v3s automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

# 15.2 The WWW Screen

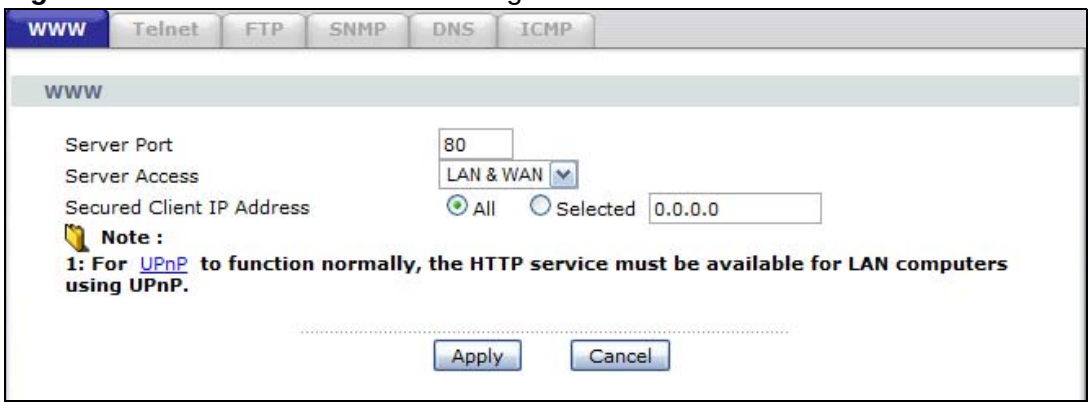
Use this screen to specify how to connect to the P-660H-T1v3s from a web browser, such as Internet Explorer.

Note: If you disable the **WWW** service in the **Remote MGMT > WWW** screen, then the P-660H-T1v3s blocks all HTTP connection attempts.

## 15.2.1 Configuring the WWW Screen

Click **Advanced > Remote MGMT** to display the **WWW** screen.

**Figure 62** Advanced > Remote Management > WWW



The following table describes the labels in this screen.

**Table 44** Advanced > Remote Management > WWW

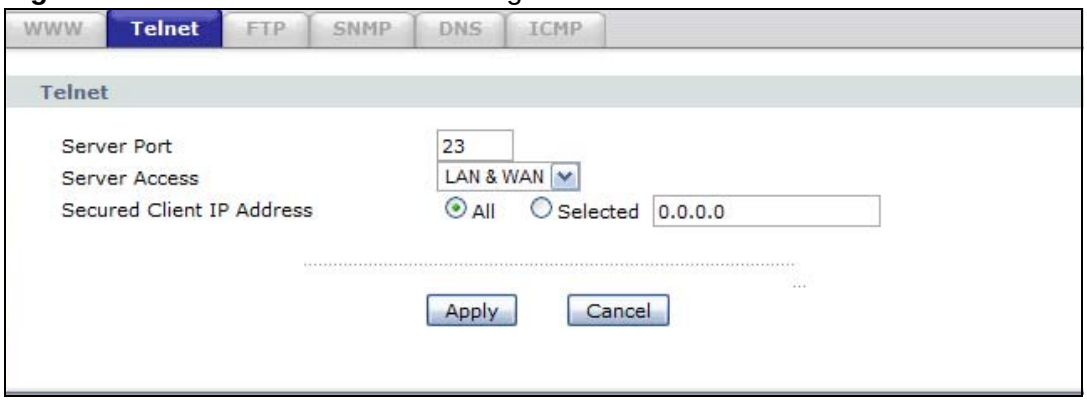
| LABEL | DESCRIPTION |
|---|---|
| Server Port | You may change the server port number for a service, if needed. However, you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the P-660H-T1v3s using this service. |
| Secured Client IP Address | A secured client is a “trusted” computer that is allowed to communicate with the P-660H-T1v3s using this service.<br>Select **All** to allow any computer to access the P-660H-T1v3s using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the P-660H-T1v3s using this service. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 15.3 The Telnet Screen

You can use Telnet to access the P-660H-T1v3s’s command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click **Advanced > Remote MGMT** > **Telnet** tab to display the screen as shown.

**Figure 63** Advanced > Remote Management > Telnet



The following table describes the labels in this screen.

**Table 45** Advanced > Remote Management > Telnet

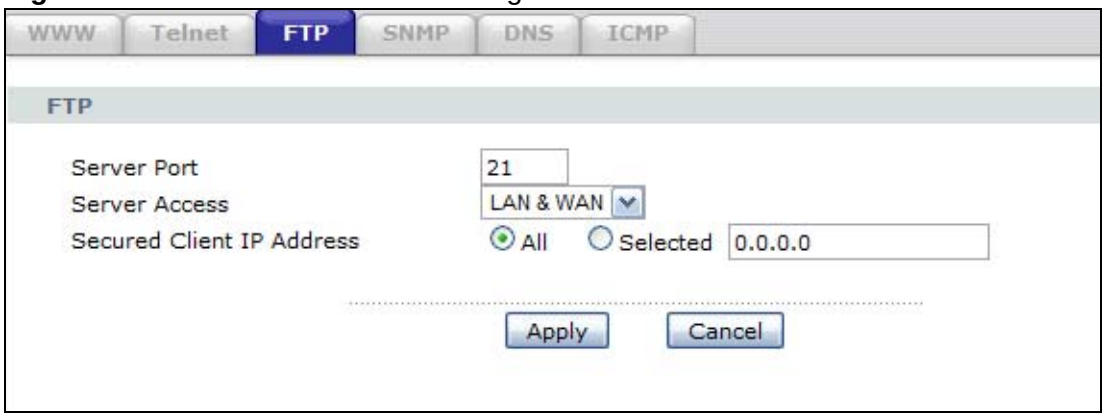
| LABEL | DESCRIPTION |
|---|---|
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the P-660H-T1v3s using this service. |
| Secured Client IP Address | A secured client is a “trusted” computer that is allowed to communicate with the P-660H-T1v3s using this service.<br>Select **All** to allow any computer to access the P-660H-T1v3s using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the P-660H-T1v3s using this service. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 15.4 The FTP Screen

You can use FTP (File Transfer Protocol) to upload and download the P-660H-T1v3s’s firmware and configuration files. Please see the User’s Guide chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

Use this screen to specify which interfaces allow FTP access and from which IP address the access can come. To change your P-660H-T1v3s’s FTP settings, click **Advanced > Remote MGMT** > **FTP**. The screen appears as shown.

**Figure 64** Advanced > Remote Management > FTP



The following table describes the labels in this screen.

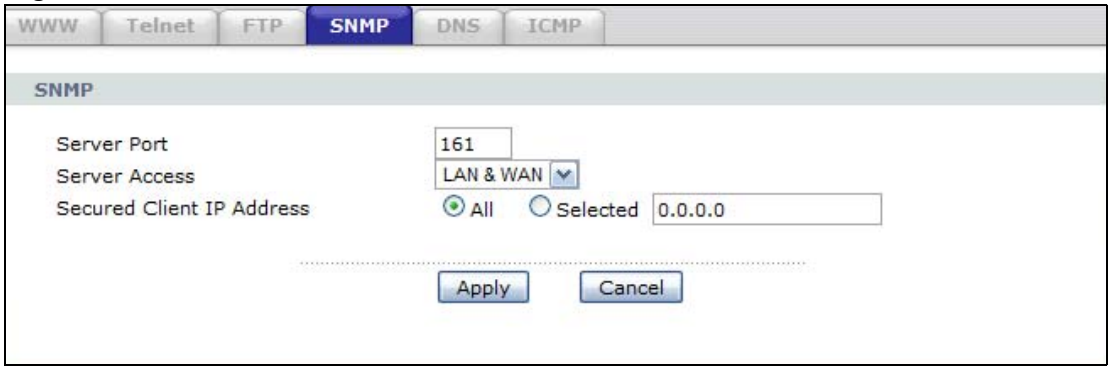
**Table 46** Advanced > Remote Management > FTP

| LABEL | DESCRIPTION |
|---|---|
| Port | You may change the server port number for a service, if needed. However, you must use the same port number in order to use that service for remote management. |
| Access Status | Select the interface(s) through which a computer may access the P-660H-T1v3s using this service. |
| Secured Client IP | A secured client is a “trusted” computer that is allowed to communicate with the P-660H-T1v3s using this service.<br>Select **All** to allow any computer to access the P-660H-T1v3s using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the P-660H-T1v3s using this service. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 15.5 The SNMP Screen

SNMP is a popular management protocol defined by the Internet community for TCP/IP networks. It is a communication protocol for collecting information from devices on the network. Click **Advanced > Remote MGMT > SNMP** to set up SNMP access for your P-660H-T1v3s.

**Figure 65** Advanced > Remote MGMT > SNMP



The following table describes the labels in this screen.

**Table 47** Advanced > Remote MGMT > SNMP

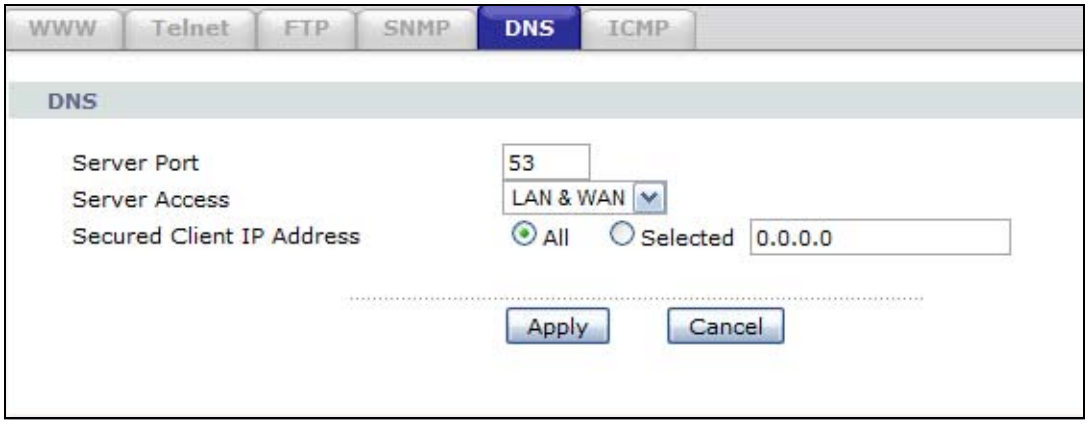
| LABEL | DESCRIPTION |
|---|---|
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the P-660H-T1v3s using this service. |
| Secured Client IP Address | A secured client is a "trusted" computer that is allowed to communicate with the P-660H-T1v3s using this service.<br>Select **All** to allow any computer to access the P-660H-T1v3s using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the P-660H-T1v3s using this service. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

# 15.6 The DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to Chapter 7 on page 89 for background information.

Use this screen to set from which IP address the P-660H-T1v3s will accept DNS queries and on which interface it can send them your P-660H-T1v3s's DNS settings. This feature is not available when the P-660H-T1v3s is set to bridge mode. Click **Advanced > Remote MGMT** > **DNS** to change your P-660H-T1v3s's DNS settings.

**Figure 66** Advanced > Remote Management > DNS



The following table describes the labels in this screen.

**Table 48** Advanced > Remote Management > DNS

| LABEL | DESCRIPTION |
|---|---|
| Server Port | The DNS service port number is 53 and cannot be changed here. |
| Server Access | Select the interface(s) through which a computer may send DNS queries to the P-660H-T1v3s. |
| Secured Client IP Address | A secured client is a “trusted” computer that is allowed to send DNS queries to the P-660H-T1v3s.<br>Select **All** to allow any computer to send DNS queries to the P-660H-T1v3s.<br>Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the P-660H-T1v3s. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 15.7 The ICMP Screen

To change your P-660H-T1v3s's security settings, click **Advanced > Remote MGMT** > **ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your P-660H-T1v3s, an ICMP response packet is automatically returned. This allows the outside user to know the P-660H-T1v3s exists. Your P-660H-T1v3s supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your P-660H-T1v3s when unsupported ports are probed.

Note: If you want your device to respond to pings and requests for unauthorized services, you may also need to configure the firewall anti probing settings to match.

**Figure 67** Advanced > Remote Management > ICMP

The following table describes the labels in this screen.

**Table 49** Advanced > Remote Management > ICMP

| LABEL | DESCRIPTION |
|---|---|
| ICMP | Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user. |
| Respond to Ping on | The P-660H-T1v3s will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests. |
| Do not respond to requests for unauthorized services | Select this option to prevent hackers from finding the P-660H-T1v3s by probing for unused ports. If you select this option, the P-660H-T1v3s will not respond to port request(s) for unused ports, thus leaving the unused ports and the P-660H-T1v3s unseen. If this option is not selected, the P-660H-T1v3s will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports.<br><br>Note that the probing packets must first traverse the P-660H-T1v3s's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the P-660H-T1v3s reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 16

# Universal Plug-and-Play (UPnP)

## 16.1 Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

### 16.1.1 What You Can Do in the UPnP Screen

Use the **UPnP** screen (Section 16.2 on page 163) to enable UPnP on the P-660H-T1v3s and allow UPnP-enabled applications to automatically configure the P-660H-T1v3s.

### 16.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

#### Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

#### NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses

- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

## Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the P-660H-T1v3s allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

## UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

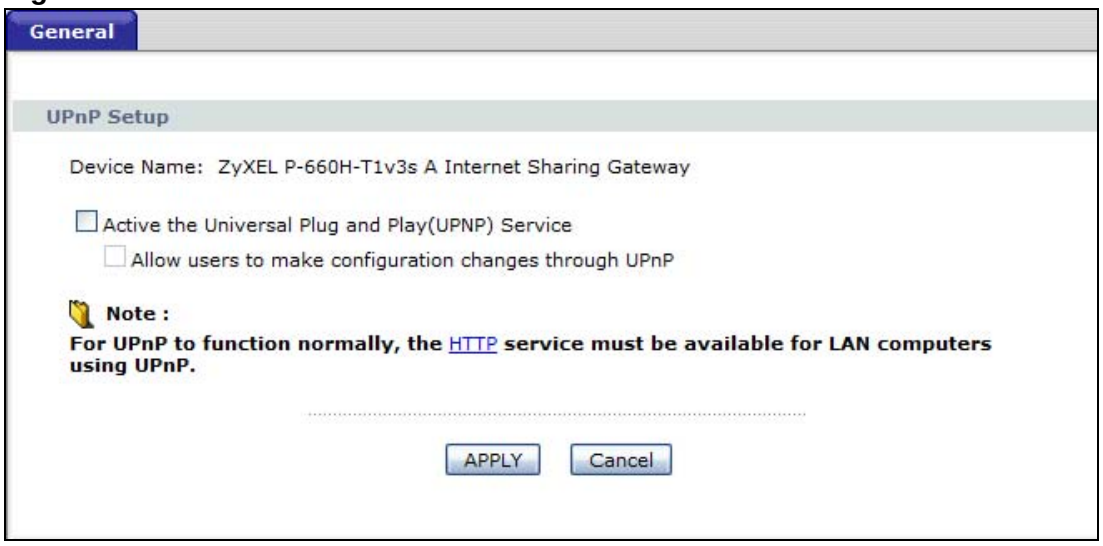
See the following sections for examples of installing and using UPnP.

# 16.2 The UPnP Screen

Use the following screen to configure the UPnP settings on your P-660H-T1v3s. Click **Advanced > UPnP** to display the screen shown next.

See Section 16.1 on page 161 for more information.

**Figure 68** Advanced > UPnP > General


General
UPnP Setup
Device Name: ZyXEL P-660H-T1v3s A Internet Sharing Gateway
Active the Universal Plug and Play(UPNP) Service
Allow users to make configuration changes through UPnP
Note :
For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
APPLY
Cancel

The following table describes the fields in this screen.

**Table 50** Advanced > UPnP > General

| LABEL | DESCRIPTION |
|---|---|
| Active the Universal Plug and Play (UPnP) Feature | Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the P-660H-T1v3s's IP address (although you must still enter the password to access the web configurator). |
| Allow users to make configuration changes through UPnP | Select this check box to allow UPnP-enabled applications to automatically configure the P-660H-T1v3s so that they can communicate through the P-660H-T1v3s, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

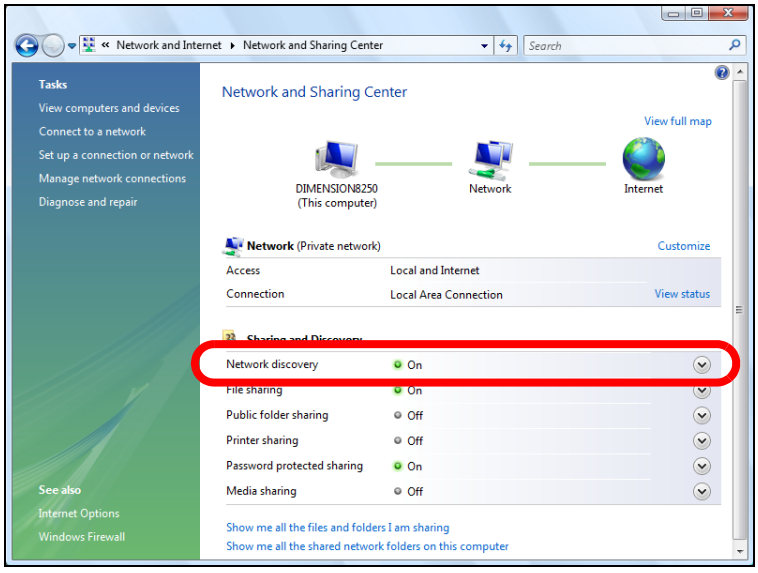
## 16.2.1 Installing UPnP in Windows

This section shows you how to configure or install UPnP in Windows.

### 16.2.1.1 Windows 7

Windows 7 already has UPnP installed. To enable it:

1. Click **Start > Control Panel** and select **Network and Internet**.
2. Click **Network and Sharing Center**.
3. In the **Network and Sharing** window, set **Network Discovery** to **On**. This activates the UPnP feature in Windows 7



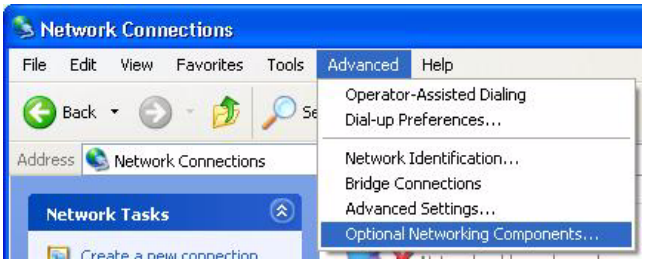
### 16.2.1.2 Windows XP

To install the UPnP in Windows XP:

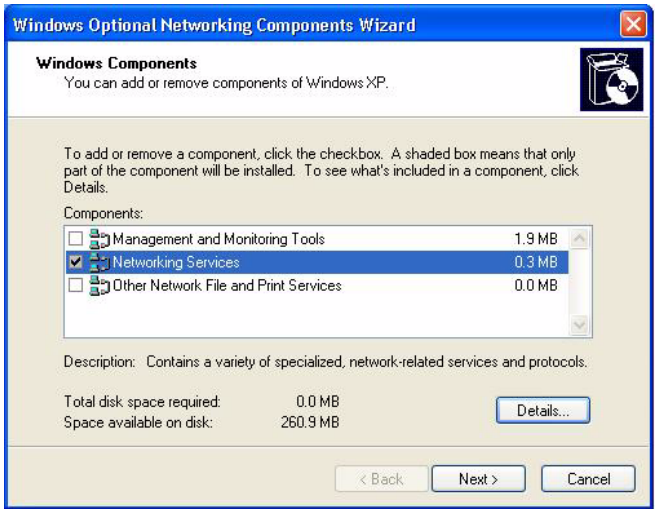
1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

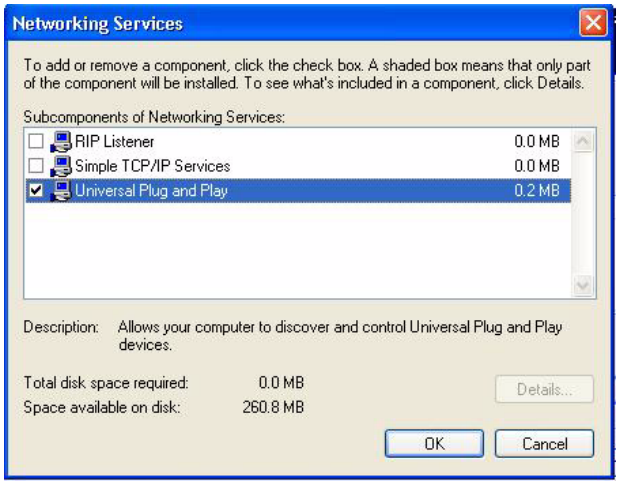
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.




4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

## 16.2.2 Using UPnP in Windows XP

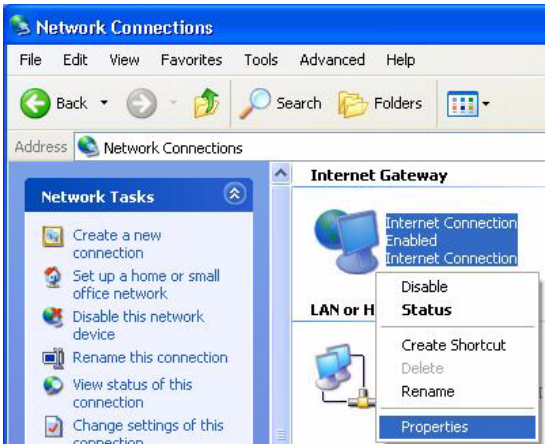
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the P-660H-T1v3s.

Make sure the computer is connected to a LAN port of the P-660H-T1v3s. Turn on your computer and the P-660H-T1v3s.

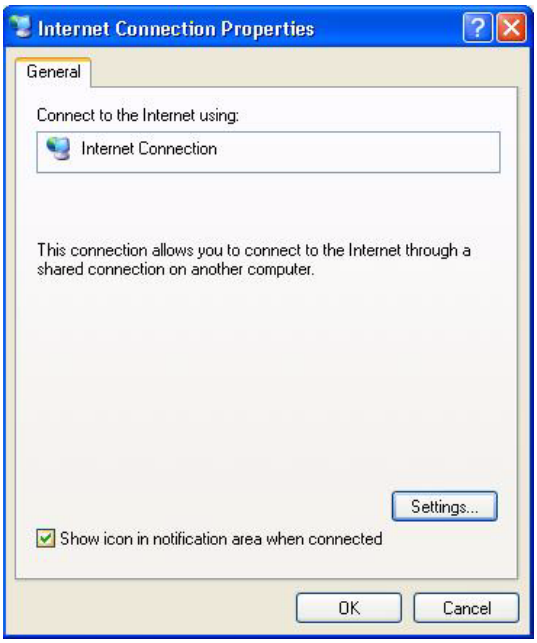
### 16.2.2.1 Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

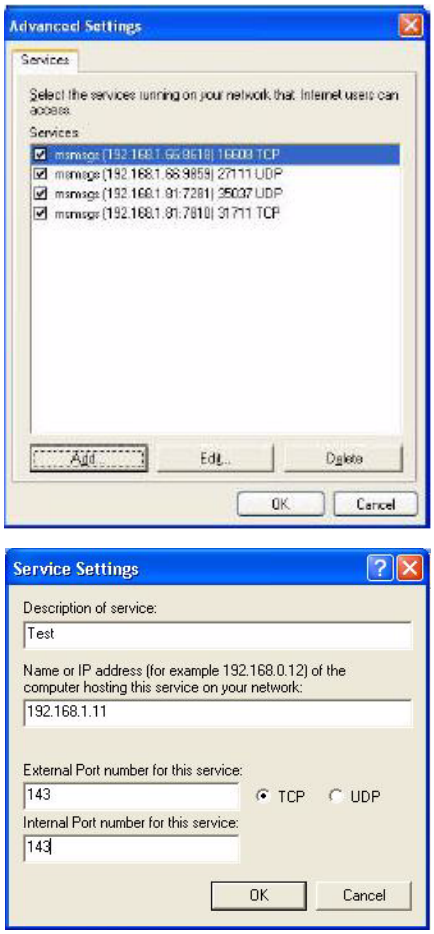
2 Right-click the icon and select **Properties**.




3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.


Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.




5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

7 Double-click on the icon to display your current Internet connection status.

## 16.2.2.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the P-660H-T1v3s without finding out the IP address of the P-660H-T1v3s first. This comes helpful if you do not know the IP address of the P-660H-T1v3s.

Follow the steps below to access the web configurator.

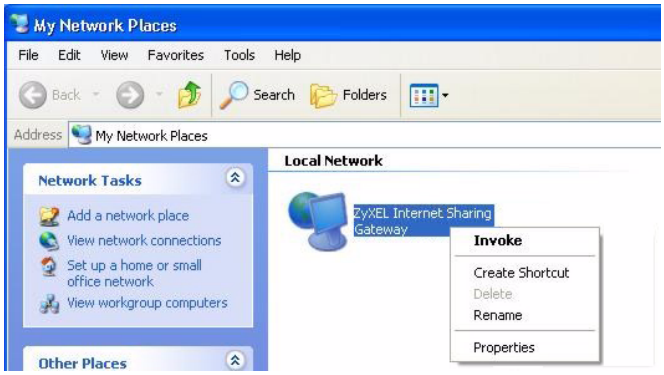
1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your P-660H-T1v3s and select **Invoke**. The web configurator login screen displays.




6 Right-click on the icon for your P-660H-T1v3s and select **Properties**. A properties window displays with basic information about the P-660H-T1v3s.

# 17

# System Settings

## 17.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

### 17.1.1 What You Can Do in the System Settings Screens

- Use the **General** screen (Section 17.2 on page 172) to configure system settings.
- Use the **Time Setting** screen (Section 17.3 on page 173) to set the system time.

### 17.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

#### DHCP

DHCP (Dynamic Host Configuration Protocol) is a method of allocating IP addresses to devices on a network from a DHCP Server. Often your ISP or a router on your network performs this function.

#### LAN

A LAN (local area network) is typically a network which covers a small area, made up of computers and other devices which share resources such as Internet access, printers etc.

# 17.2 The General Screen

Use this screen to configure system settings such as the system and domain name, inactivity timeout interval and system password.

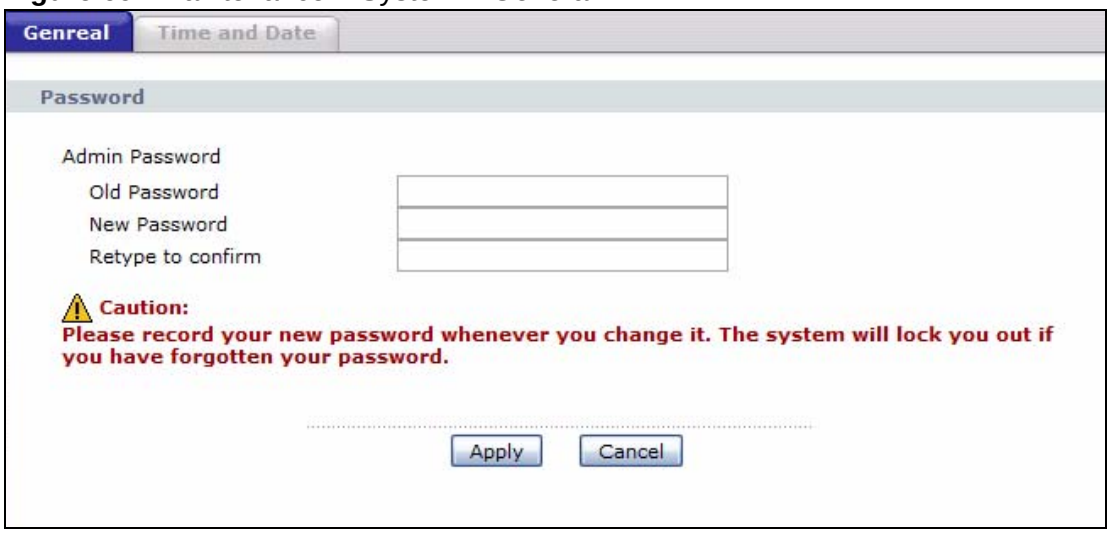
The **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

To find your computer in Windows XP, right-click over **My Computer** and select **Properties**. Next, click the **Computer Name** tab.

In Windows 7, open your **Start** menu, right-click over the **Computer** item, and select **Properties**.

Click **Maintenance > System** to open the **General** screen.

**Figure 69** Maintenance > System > General




The following table describes the labels in this screen.

**Table 51** Maintenance > System > General

| LABEL | DESCRIPTION |
|---|---|
| Admin Password | |
| Old Password | Type the default password or the existing password you use to access the system in this field. |
| New Password | Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the P-660H-T1v3s. |
| Retype to confirm | Type the new password again for confirmation. |

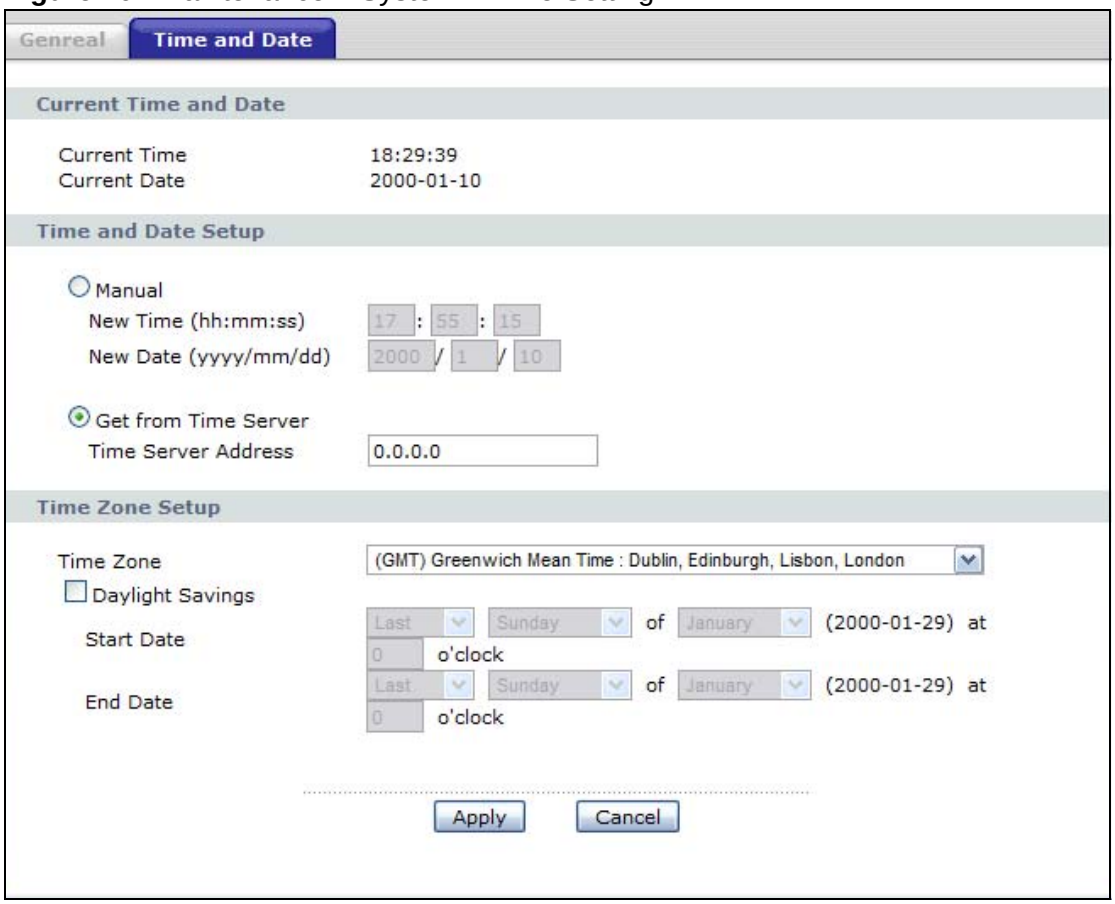
**Table 51** Maintenance > System > General

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 17.3 The Time and Date Screen

Use this screen to configure the P-660H-T1v3s's time based on your local time zone. To change your P-660H-T1v3s's time and date, click **Maintenance > System > Time and Date**. The screen appears as shown.

**Figure 70** Maintenance > System > Time Setting



The following table describes the fields in this screen.

**Table 52** Maintenance > System > Time and Date

| LABEL | DESCRIPTION |
|---|---|
| Current Time | |
| Current Time | This field displays the time of your P-660H-T1v3s.<br>Each time you reload this page, the P-660H-T1v3s synchronizes the time with the time server. |
| Current Date | This field displays the date of your P-660H-T1v3s.<br>Each time you reload this page, the P-660H-T1v3s synchronizes the date with the time server. |
| Time and Date Setup | |
| Manual | Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it. |
| New Time<br>(hh:mm:ss) | This field displays the last updated time from the time server or the last time configured manually.<br>When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**. |
| New Date<br>(yyyy/mm/dd) | This field displays the last updated date from the time server or the last date configured manually.<br>When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**. |
| Get from Time Server | Select this radio button to have the P-660H-T1v3s get the time and date from the time server you specified below. |
| Time Protocol | Select the time service protocol that your time server sends when you turn on the P-660H-T1v3s. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.<br>The main difference between them is the format.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>The default, **NTP (RFC 1305)**, is similar to Time (RFC 868). |
| Time Server Address | Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information. |
| Time Zone Setup | |
| Time Zone | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |

**Table 52** Maintenance > System > Time and Date (continued)

| LABEL | DESCRIPTION |
|---|---|
| Daylight Savings | Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.<br><br>Select this option if you use Daylight Saving Time. |
| Start Date | Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples:<br><br>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field.<br><br>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End Date | Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples:<br><br>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field.<br><br>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 18 Logs

## 18.1 Overview

This chapter contains information about configuring general log settings and viewing the P-660H-T1v3s's logs.

The web configurator allows you to choose which categories of events and/or alerts to have the P-660H-T1v3s log and then display the logs or have the P-660H-T1v3s send them to an administrator (as e-mail) or to a syslog server.

### 18.1.1 What You Can Do in the Log Screens

Use the **System Log** screen (Section 18.2 on page 178) to see the logs for the categories that you selected in the **Log Settings** screen.

### 18.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

#### Alerts

An alert is a message that is enabled as soon as the event occurs. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

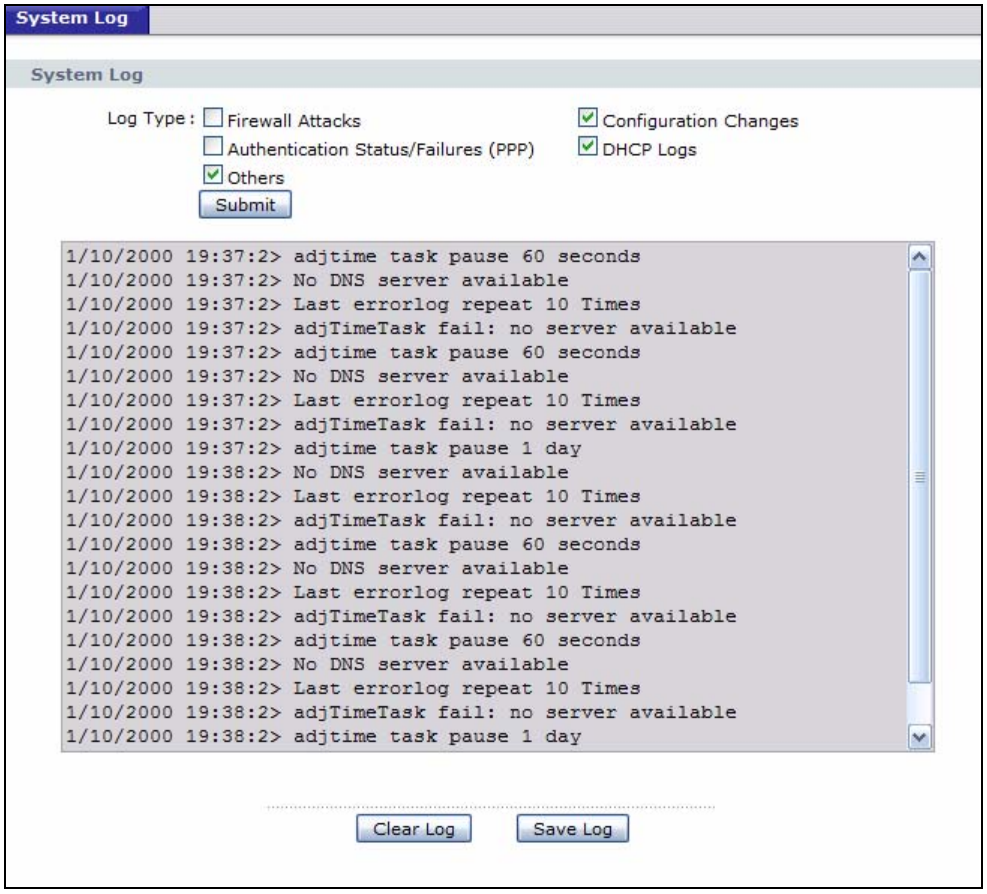
#### Logs

A log is a message about an event that occurred on your P-660H-T1v3s. For example, when someone logs in to the P-660H-T1v3s, you can set a schedule for how often logs should be enabled, or sent to a syslog server.

# 18.2 The System Log Screen

Use the **System Log** screen to see the logs for the categories that you select. Click **Maintenance > Logs** to open this screen.

**Figure 71** Maintenance > Logs > View Log


System Log
System Log
Log Type :
Firewall Attacks
Configuration Changes
Authentication Status/Failures (PPP)
DHCP Logs
Others
Submit
1/10/2000 19:37:2> adjtime task pause 60 seconds
1/10/2000 19:37:2> No DNS server available
1/10/2000 19:37:2> Last errorlog repeat 10 Times
1/10/2000 19:37:2> adjTimeTask fail: no server available
1/10/2000 19:37:2> adjtime task pause 60 seconds
1/10/2000 19:37:2> No DNS server available
1/10/2000 19:37:2> Last errorlog repeat 10 Times
1/10/2000 19:37:2> adjTimeTask fail: no server available
1/10/2000 19:37:2> adjtime task pause 1 day
1/10/2000 19:38:2> No DNS server available
1/10/2000 19:38:2> Last errorlog repeat 10 Times
1/10/2000 19:38:2> adjTimeTask fail: no server available
1/10/2000 19:38:2> adjtime task pause 60 seconds
1/10/2000 19:38:2> No DNS server available
1/10/2000 19:38:2> Last errorlog repeat 10 Times
1/10/2000 19:38:2> adjTimeTask fail: no server available
1/10/2000 19:38:2> adjtime task pause 60 seconds
1/10/2000 19:38:2> No DNS server available
1/10/2000 19:38:2> Last errorlog repeat 10 Times
1/10/2000 19:38:2> adjTimeTask fail: no server available
1/10/2000 19:38:2> adjtime task pause 1 day
Clear Log
Save Log

The following table describes the fields in this screen.

**Table 53** Maintenance > Logs > View Log

| LABEL | DESCRIPTION |
|---|---|
| Log Type | Select the type of log to display in the system log window. |
| Submit | Click this after selecting the **Log Type** and to populate the log window with any applicable log messages. |
| Clear Log | Click this to clear the log window of any system log messages. |
| Save Log | Click this to the system log to your computer. A *.log files appears in your browser window, which you can save to your computer as a plain text file. |

# 19 Tools

## 19.1 Overview

This chapter explains how to upload new firmware, manage configuration files and restart your P-660H-T1v3s.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

**Only use firmware for your device's specific model. Refer to the label on the bottom of your P-660H-T1v3s.**

### 19.1.1 What You Can Do in the Tool Screens

- Use the **Firmware Upgrade** screen (Section 19.2 on page 187) to upload firmware to your device.
- Use the **Configuration** screen (Section 19.3 on page 189) to backup and restore device configurations. You can also reset your device settings back to the factory default.
- Use the **Restart** screen (Section 19.4 on page 192) to restart your ZyXEL device.

## 19.1.2 What You Need To Know About Tools

### Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a “rom” filename extension. Once you have customized the P-660H-T1v3s's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. Find this firmware at www.zyxel.com.With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the P-660H-T1v3s.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file “config.cfg”.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the P-660H-T1v3s only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the P-660H-T1v3s and the external filename refers to the filename not on the P-660H-T1v3s, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

**Table 54** Filename Conventions

| FILE TYPE | INTERNAL NAME | EXTERNAL NAME | DESCRIPTION |
|---|---|---|---|
| Configuration File | Rom-0 | This is the configuration filename on the P-660H-T1v3s. Uploading the rom-0 file replaces the entire ROM file system, including your P-660H-T1v3s configurations, system-related data (including the default password), the error log and the trace log. | *.rom |
| Firmware | Ras | This is the generic name for the ZyNOS firmware on the P-660H-T1v3s. | *.bin |

### FTP Restrictions

FTP will not work when:

1. The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).
2. You have disabled the FTP service in the **Remote Management** screen.
3. The IP you entered in the Secured Client IP field does not match the client IP. If it does not match, the device will disallow the FTP session.

## 19.1.3 Before You Begin

- Ensure you have either created a firewall rule to allow access from the WAN or turned the firewall off, otherwise the FTP will not function.
- Make sure the FTP service has not been disabled in the Remote Management screen.

## 19.1.4 Tool Examples

### Using FTP or TFTP to Restore Configuration

This example shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

**Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device. When the Restore Configuration process is complete, the device automatically restarts.**

### Restore Using FTP Session Example

**Figure 72** Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to Section 19.1.2 on page 180 to read about configurations that disallow TFTP and FTP over WAN.

### FTP and TFTP Firmware and Configuration File Uploads

These examples show you how to upload firmware and configuration files.

**Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device.**

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

### FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your device.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer files from the computer to the device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

### FTP Session Example of Firmware File Upload

**Figure 73** FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed in this chapter.

Refer to Section 19.1.2 on page 180 to read about configurations that disallow TFTP and FTP over WAN.

### TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Enter the command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.
3. Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.
4. Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is “ras”.

   Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For

UNIX, use “get” to transfer from the device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

### TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the device’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

### Using the FTP Commands to Back Up Configuration

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your P-660H-T1v3s.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “get” to transfer files from the P-660H-T1v3s to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the P-660H-T1v3s to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

### FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your device's configuration onto your computer.

**Figure 74** FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

### Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

**Table 55** General Commands for GUI-based FTP Clients

| COMMAND | DESCRIPTION |
|---|---|
| Host Address | Enter the address of the host server. |
| Login Type | Anonymous.<br>This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.<br>Normal.<br>The server requires a unique User ID and Password to login. |
| Transfer Type | Transfer files in either ASCII (plain text format) or in binary mode. |
| Initial Remote Directory | Specify the default remote directory (path). |
| Initial Local Directory | Specify the default local directory (path). |

### Backup Configuration Using TFTP

The P-660H-T1v3s supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the P-660H-T1v3s and log in. Because TFTP does not have any security checks, the P-660H-T1v3s records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Enter command "sys stdio 0" to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute management idle timeout (default) when the file transfer is complete.

3 Launch the TFTP client on your computer and connect to the P-660H-T1v3s. Set the transfer mode to binary before starting data transfer.

4 Use the TFTP client (see the example below) to transfer files between the P-660H-T1v3s and the computer. The file name for the configuration file is "rom-0" (rom-zero, not capital o).

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the P-660H-T1v3s to the computer and "binary" to set binary transfer mode.

### TFTP Command Configuration Backup Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the P-660H-T1v3s IP address, "get" transfers the file source on the P-660H-T1v3s (rom-0, name of the configuration file on the P-660H-T1v3s) to the file destination on the computer and renames it config.rom.

### Configuration Backup Using GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

**Table 56** General Commands for GUI-based TFTP Clients

| COMMAND | DESCRIPTION |
|---|---|
| Host | Enter the IP address of the P-660H-T1v3s. 192.168.1.1 is the P-660H-T1v3s's default IP address when shipped. |
| Send/ Fetch | Use "Send" to upload the file to the P-660H-T1v3s and "Fetch" to back up the file on your computer. |
| Local File | Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer. |
| Remote File | This is the filename on the P-660H-T1v3s. The filename for the firmware is "ras" and for the configuration file, is "rom-0". |

**Table 56** General Commands for GUI-based TFTP Clients (continued)

| COMMAND | DESCRIPTION |
|---|---|
| Binary | Transfer the file in binary mode. |
| Abort | Stop transfer of the file. |

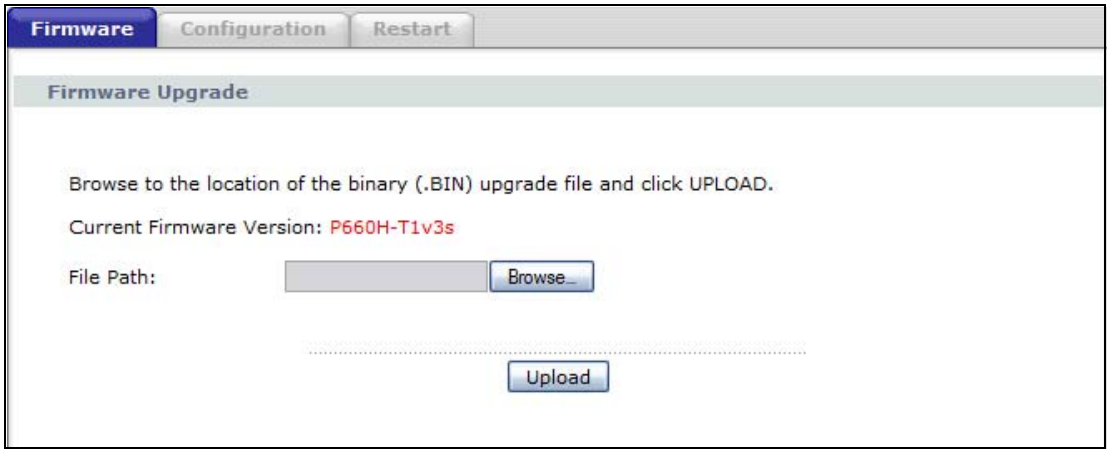
Refer to Section 19.1.2 on page 180 to read about configurations that disallow TFTP and FTP over WAN.

# 19.2 The Firmware Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your P-660H-T1v3s. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Section 19.1.4 on page 181 for upgrading firmware using FTP/TFTP commands.

**Do NOT turn off the P-660H-T1v3s while firmware upload is in progress!**

**Figure 75** Maintenance > Tools > Firmware




The following table describes the labels in this screen.

**Table 57** Maintenance > Tools > Firmware

| LABEL | DESCRIPTION |
|---|---|
| Current Firmware Version | This is the present Firmware version and the date created. |
| File Path | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |

**Table 57** Maintenance > Tools > Firmware (continued)

| LABEL | DESCRIPTION |
|---|---|
| Browse... | Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Upload | Click this to begin the upload process. This process may take up to two minutes. |

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the P-660H-T1v3s again.

**Figure 76** Firmware Upload In Progress

ZyXEL
Firmware Upload In Progress
Do not Turn Off the Device.
Please Wait ...
Please wait for the device to finish restarting(PWR LED is on steady). This should take about two minutes.
To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status menu.

The P-660H-T1v3s automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 77** Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

**Figure 78** Error Message

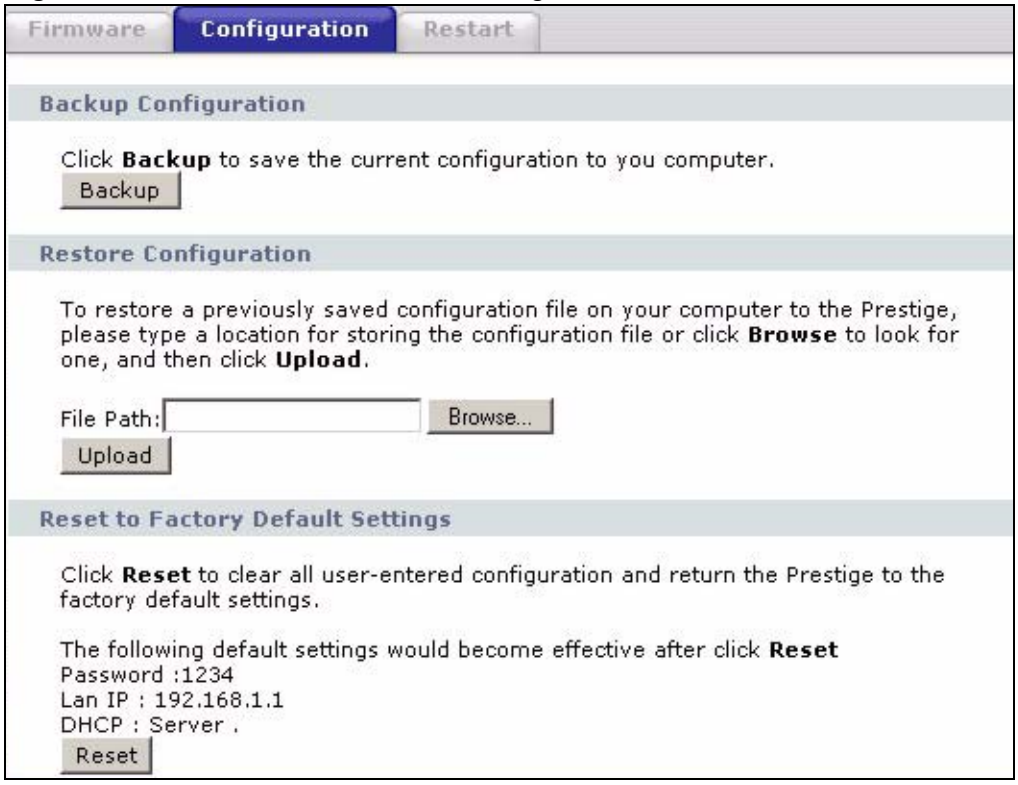
System Upload
Firmware upload error!
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.
Return

# 19.3 The Configuration Screen

See Section 19.1.4 on page 181 for transferring configuration files using FTP/TFTP commands.

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

**Figure 79** Maintenance > Tools > Configuration


Firmware
Configuration
Restart
Backup Configuration
Click Backup to save the current configuration to you computer.
Backup
Restore Configuration
To restore a previously saved configuration file on your computer to the Prestige, please type a location for storing the configuration file or click Browse to look for one, and then click Upload.
File Path:
Browse...
Upload
Reset to Factory Default Settings
Click Reset to clear all user-entered configuration and return the Prestige to the factory default settings.
The following default settings would become effective after click Reset
Password :1234
Lan IP : 192.168.1.1
DHCP : Server .
Reset

## Backup Configuration

Backup Configuration allows you to back up (save) the P-660H-T1v3s's current configuration to a file on your computer. Once your P-660H-T1v3s is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the P-660H-T1v3s's current configuration to your computer.

## Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your P-660H-T1v3s.

**Table 58** Restore Configuration

| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |
| Browse... | Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them. |
| Upload | Click this to begin the upload process. |

**Do not turn off the P-660H-T1v3s while configuration file upload is in progress.**

After you see a "restore configuration successful" screen, you must then wait one minute before logging into the P-660H-T1v3s again.

**Figure 80** Configuration Upload Successful

ZyXEL
Restore Configuration successful
The Router Is Rebooting Now.
Please Wait ...
The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

The P-660H-T1v3s automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 81** Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix A on page 211 for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

**Figure 82** Configuration Upload Error

System Restore
Restore configuration error!
The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.
Return

### Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the P-660H-T1v3s to its factory defaults. The following warning screen appears.

**Figure 83** Reset Warning Message

Microsoft Internet Explorer
Are you sure you want to reset the device back to the factory defaults?This will erase all of your custom configuration.
OK
Cancel

**Figure 84** Reset In Process Message

ZyXEL
Reset to Factory Default Settings
Please Wait ...
The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the device again.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your P-660H-T1v3s. Refer to Section 1.5 on page 24 for more information on the **RESET** button.

## 19.4 The Restart Screen

System restart allows you to reboot the P-660H-T1v3s remotely without turning the power off. You may need to do this if the P-660H-T1v3s hangs, for example.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the P-660H-T1v3s reboot. This does not affect the P-660H-T1v3s's configuration.

**Figure 85** Maintenance > Tools >Restart

Firmware
Configuration
Restart
System Reboot
Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.
Restart

# 20 Diagnostic

## 20.1 Overview

These read-only screens display information to help you identify problems with the P-660H-T1v3s.

### 20.1.1 What You Can Do in the Diagnostic Screens

- Use the **General Diagnostic** screen (Section 20.2 on page 193) to ping an IP address.
- Use the **DSL Line Diagnostic** screen (Section 20.3 on page 194) to view the DSL line statistics and reset the ADSL line.

## 20.2 The General Diagnostic Screen

Use this screen to ping an IP address. Click **Maintenance > Diagnostic** to open the screen shown next.

**Figure 86** Maintenance > Diagnostic > General

The following table describes the fields in this screen.

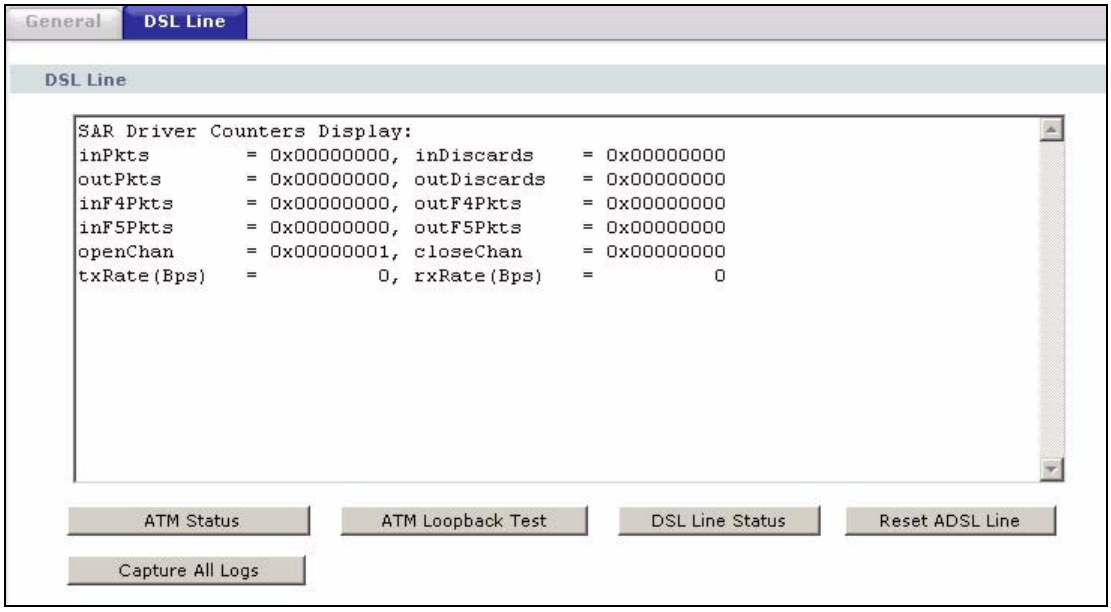
**Table 59** Maintenance > Diagnostic > General

| LABEL | DESCRIPTION |
|---|---|
| TCP/IP Address | Type the IP address of a computer that you want to ping in order to test a connection. |
| Ping | Click this to ping the IP address that you entered. |

# 20.3 The DSL Line Diagnostic Screen

Use this screen to view the DSL line statistics and reset the ADSL line. Click **Maintenance > Diagnostic** > **DSL Line** to open the screen shown next.

**Figure 87** Maintenance > Diagnostic > DSL Line



The following table describes the fields in this screen.

**Table 60** Maintenance > Diagnostic > DSL Line

| LABEL | DESCRIPTION |
|---|---|
| ATM Status | Click this to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed.<br><br>The (Segmentation and Reassembly) SAR driver translates packets into ATM cells. It also receives ATM cells and reassembles them into packets.<br><br>These counters are set back to zero whenever the device starts up.<br><br>**inPkts** is the number of good ATM cells that have been received.<br><br>**inDiscards** is the number of received ATM cells that were rejected.<br><br>**outPkts** is the number of ATM cells that have been sent.<br><br>**outDiscards** is the number of ATM cells sent that were rejected.<br><br>**inF4Pkts** is the number of ATM Operations, Administration, and Management (OAM) F4 cells that have been received. See ITU recommendation I.610 for more on OAM for ATM.<br><br>**outF4Pkts** is the number of ATM OAM F4 cells that have been sent.<br><br>**inF5Pkts** is the number of ATM OAM F5 cells that have been received.<br><br>**outF5Pkts** is the number of ATM OAM F5 cells that have been sent.<br><br>**openChan** is the number of times that the P-660H-T1v3s has opened a logical DSL channel.<br><br>**closeChan** is the number of times that the P-660H-T1v3s has closed a logical DSL channel.<br><br>**txRate** is the number of bytes transmitted per second.<br><br>**rxRate** is the number of bytes received per second. |
| ATM Loopback Test | Click this to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The P-660H-T1v3s sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the P-660H-T1v3s. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network. |

**Table 60** Maintenance > Diagnostic > DSL Line (continued)

| LABEL | DESCRIPTION |
|---|---|
| DSL Line Status | Click this to view statistics about the DSL connections.<br><br>**noise margin downstream** is the signal to noise ratio for the downstream part of the connection (coming into the P-660H-T1v3s from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is.<br><br>**output power upstream** is the amount of power (in decibels) that the P-660H-T1v3s is using to transmit to the ISP.<br><br>**attenuation downstream** is the reduction in amplitude (in decibels) of the DSL signal coming into the P-660H-T1v3s from the ISP.<br><br>Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT.<br><br>The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels. |
| Reset ADSL Line | Click this to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:<br><br>`"Start to reset ADSL`<br><br>`Loading ADSL modem F/W...`<br><br>`Reset ADSL Line Successfully!"` |
| Capture All Logs | Click this to display information and statistics about your P-660H-T1v3s's ATM statistics, DSL connection statistics, DHCP settings, firmware version, WAN and gateway IP address, VPI/VCI and LAN IP address. |

# 21

# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.


- Power, Hardware Connections, and LEDs
- P-660H-T1v3s Access and Login
-
- Internet Access


## 21.1 Power, Hardware Connections, and LEDs

### The P-660H-T1v3s does not turn on. None of the LEDs turn on.

1. Make sure the P-660H-T1v3s is turned on.
2. Make sure you are using the power adaptor or cord included with the P-660H-T1v3s.
3. Make sure the power adaptor or cord is connected to the P-660H-T1v3s and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the P-660H-T1v3s off and on.
5. If the problem continues, contact the vendor.

### One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.4 on page 23.

2 Check the hardware connections.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the P-660H-T1v3s off and on.

5 If the problem continues, contact the vendor.

## 21.2 P-660H-T1v3s Access and Login

### I forgot the IP address for the P-660H-T1v3s.

1 The default IP address is **192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the P-660H-T1v3s by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the P-660H-T1v3s (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 24.

### I forgot the password.

1 The default admin password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 24.

### I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.

- If you changed the IP address (Section 7.2 on page 91), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the P-660H-T1v3s.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix B on page 235.

4 If you disabled **Any IP** (Section 7.6.7 on page 102), make sure your computer is in the same subnet as the P-660H-T1v3s. (If you know that there are routers between your computer and the P-660H-T1v3s, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix A on page 211. Your P-660H-T1v3s is a DHCP server by default.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the P-660H-T1v3s. See Appendix A on page 211.

5 Reset the device to its factory defaults, and try to access the P-660H-T1v3s with the default IP address. See Section 1.5 on page 24.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Try to access the P-660H-T1v3s using another service, such as Telnet. If you can access the P-660H-T1v3s, check the remote management settings and firewall rules to find out why the P-660H-T1v3s does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

## I can see the **Login** screen, but I cannot log in to the P-660H-T1v3s.

1 Make sure you have entered the password correctly. The default admin password is **1234**. The field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the P-660H-T1v3s. Log out of the P-660H-T1v3s in the other session, or ask the person who is logged in to log out.

3 Turn the P-660H-T1v3s off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 21.1 on page 197.

### I cannot Telnet to the P-660H-T1v3s.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

### I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

## 21.3 Internet Access

### I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4 on page 23.

2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

4 If the problem continues, contact your ISP.

### I cannot access the Internet anymore. I had access to the Internet (with the P-660H-T1v3s), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4 on page 23.

2 Turn the P-660H-T1v3s off and on.

3 If the problem continues, contact your ISP.

## The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.4 on page 23. If the P-660H-T1v3s is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Turn the P-660H-T1v3s off and on.

3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

# 22

# Product Specifications

## 22.1 Hardware Specifications

The following table summarizes the P-660H-T1v3s's hardware features.

**Table 61** Hardware Specifications

| | |
|---|---|
| Dimensions | 180W x 127D x 37H |
| Weight | 280 g |
| Power Output | 9VDC@0.6A |
| Built-in Switch | Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports |
| DSL Port | 1 RJ-11 for Annex A<br><br>RJ11 and RJ45 dual-layout reserved for Annex B |
| LAN Ports | Four RJ-45 Ports<br><br>10/100 Mbps Fast Ethernet Switch, N-way automatic speed negotiation supported<br><br>Auto-sensing, auto-detection MDI/MDI-X |
| Restore/Reset Button | Restores factory defaults if held for 10 seconds |
| Operating Temperature | 0º C ~ 40º C |
| Storage Temperature | -20º ~ 60º C |
| Operating Humidity | 20% ~ 85% RH |
| Storage Humidity | 20% ~ 90% RH |

# 22.2 Firmware Specifications

The following table summarizes the P-660H-T1v3s's firmware features.

**Table 62** Firmware Specifications

| | |
|---|---|
| Default IP Address | 192.168.1.1 |
| Default Subnet Mask | 255.255.255.0 (24 bits) |
| Default Admin Password | 1234 |
| Static DHCP Addresses | 10 |
| Static Routes | 16 |
| Device Management | Use the web configurator to easily configure the rich range of features on the P-660H-T1v3s. |
| Firmware Upgrade | Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the P-660H-T1v3s.<br><br>Note: Only upload firmware for your specific model! |
| Configuration Backup & Restoration | Make a copy of the P-660H-T1v3s's configuration. You can put it back on the P-660H-T1v3s later if you decide to revert back to an earlier configuration. |
| Network Address Translation (NAT) | Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network. |
| Port Forwarding | If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet. |
| DHCP (Dynamic Host Configuration Protocol) | Use this feature to have the P-660H-T1v3s assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients. |
| Dynamic DNS Support | With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider. |
| IP Multicast | IP multicast is used to send traffic to a specific group of computers. The P-660H-T1v3s supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236). |
| Time and Date | Get the current time and date from an external server when you turn on your P-660H-T1v3s. You can also set the time manually. These dates and times are then used in logs. |
| Logs | Use logs for troubleshooting. You can send logs from the P-660H-T1v3s to an external syslog server. |
| Universal Plug and Play (UPnP) | A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network. |

**Table 62** Firmware Specifications (continued)

| | |
|---|---|
| Firewall | Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs. |
| Content Filtering | Content filtering allows you to block access to Internet web sites that contain key words (that you specify) in the URL. You can also schedule when to perform the filtering and give trusted LAN IP addresses unfiltered Internet access. |
| QoS (Quality of Service) | You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers. |
| Remote Management | This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the P-660H-T1v3s. |
| PPPoE Support (RFC2516) | PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers. |
| Other PPPoE Features | PPPoE idle time out<br><br>PPPoE dial on demand |
| Multiple PVC (Permanent Virtual Circuits) Support | Your device supports up to 8 Permanent Virtual Circuits (PVCs). |
| IP Alias | IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network. |
| Packet Filters | Your device's packet filtering function allows added network security and management. |

**Table 62** Firmware Specifications (continued)

| | |
|---|---|
| ADSL Standards | ANSI T1.413, Issue 2; G.dmt (G.992.1)<br>ADSL2 G.dmt.bis (G.992.3)<br>ADSL2 G.lite.bis (G.992.4)<br>ADSL2+ (G.992.5)<br>Reach-Extended ADSL (RE ADSL)<br>SRA (Seamless Rate Adaptation)<br>Auto-negotiating rate adaptation<br>ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5)<br>Multi-protocol over AAL5 (RFC2684/1483)<br>PPP over ATM AAL5 (RFC2364)<br>PPP over Ethernet for DSL connection (RFC2516)<br>VC-based and LLC-based multiplexing<br>Supports up to 8 PVCs<br>I.610 F4/F5 OAM<br>TR-067/TR-100 |

**Table 62** Firmware Specifications (continued)

| | |
|---|---|
| Other Protocol Support | PPP (Point-to-Point Protocol) link layer protocol<br>IP routing<br>DNS Proxy<br>Transparent bridging for unsupported network layer protocols<br>RIP I/RIP II<br>ICMP<br>Dynamic DNS (www.dyndns.org)<br>DHCP client/server/relay<br>ATM QoS<br>IP Multicasting IGMP v1, v2<br>IGMP Proxy<br>802.1Q/1P<br>UPnP support |
| Management | Embedded Web Configurator<br>CLI (Command Line Interpreter)<br>Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore<br>Telnet for remote management<br>Remote Management Control: Telnet, FTP, Web and DNS.<br>Remote Firmware Upgrade<br>Syslog<br>TR-069 |

# 22.3 Standards Support

The following list, which is not exhaustive, describes the standards supported in the P-660H-T1v3s.

**Table 63** Standards Supported

| STANDARD | DESCRIPTION |
|---|---|
| RFC 867 | Daytime Protocol |
| RFC 868 | Time Protocol. |
| RFC 1058 | RIP-1 (Routing Information Protocol) |
| RFC 1112 | IGMP v1 |
| RFC 1305 | Network Time Protocol (NTP version 3) |

**Table 63** Standards Supported (continued)

| STANDARD | DESCRIPTION |
|---|---|
| RFC 1483 | Multiprotocol Encapsulation over ATM Adaptation Layer 5 |
| RFC 1631 | IP Network Address Translator (NAT) |
| RFC 1661 | The Point-to-Point Protocol (PPP) |
| RFC 1723 | RIP-2 (Routing Information Protocol) |
| RFC 2236 | Internet Group Management Protocol, Version 2. |
| RFC 2364 | PPP over AAL5 (PPP over ATM over ADSL) |
| RFC 2408 | Internet Security Association and Key Management Protocol (ISAKMP) |
| RFC 2516 | A Method for Transmitting PPP Over Ethernet (PPPoE) |
| RFC 2684 | Multiprotocol Encapsulation over ATM Adaptation Layer 5. |
| RFC 2766 | Network Address Translation - Protocol |
| ANSI T1.413, Issue 2 | Asymmetric Digital Subscriber Line (ADSL) standard. |
| G dmt(G.992.1) | G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers |
| ITU G.992.1 (G.DMT) | ITU standard for ADSL using discrete multitone modulation. |
| ITU G.992.2 (G. Lite) | ITU standard for ADSL using discrete multitone modulation. |
| ITU G.992.3 (G.dmt.bis) | ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates. |
| ITU G.992.4 (G.lite.bis) | ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates. |
| ITU G.992.5 (ADSL2+) | ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits. |
| Microsoft PPTP | MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol) |
| MBM v2 | Media Bandwidth Management v2 |
| RFC 2383 | ST2+ over ATM Protocol Specification - UNI 3.1 Version |
| TR-069 | TR-069 DSL Forum Standard for CPE Wan Management. |
| 1.363.5 | Compliant AAL5 SAR (Segmentation And Re-assembly) |

# PART III
# Appendices and Index

Note: The appendices provide general information. Some details may not apply to your P-660H-T1v3s.

A

# Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

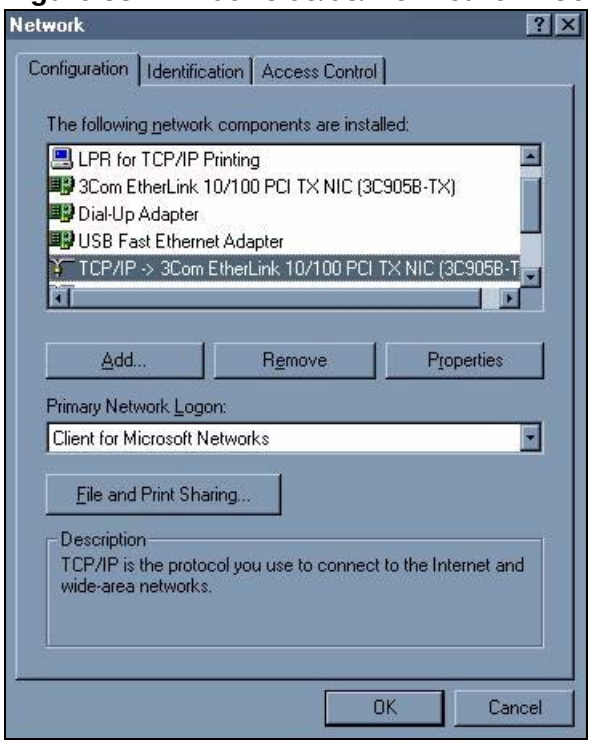
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the P-660H-T1v3s's LAN port.

# Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 88** WIndows 95/98/Me: Network: Configuration




## Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.

2 Select **Adapter** and then click **Add**.

3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.

2 Select **Protocol** and then click **Add**.

3 Select **Microsoft** from the list of **manufacturers**.

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

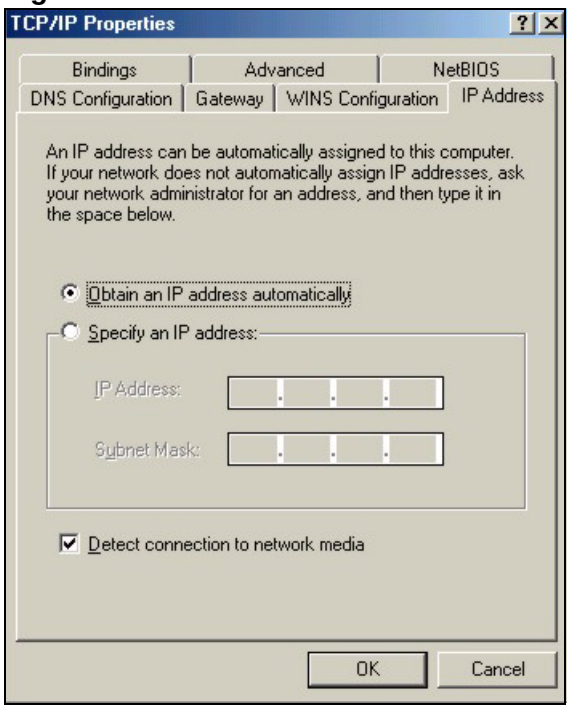
## Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

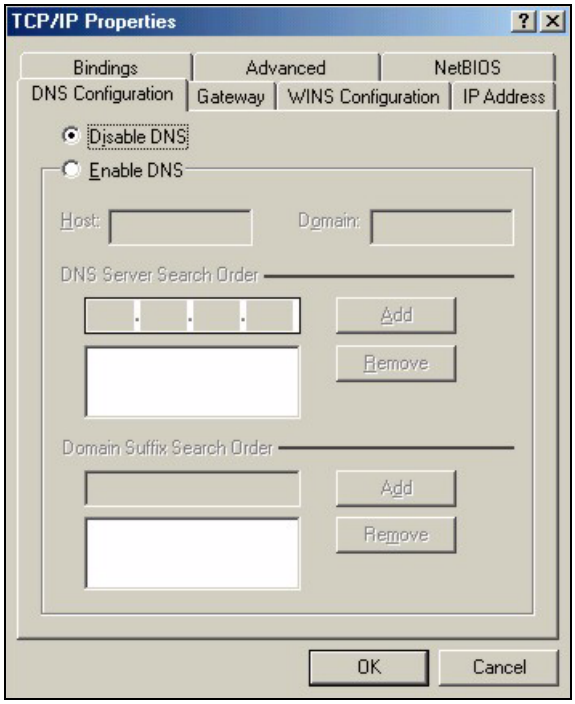
**Figure 89** Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 90** Windows 95/98/Me: TCP/IP Properties: DNS Configuration




4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your P-660H-T1v3s and restart your computer when prompted.

## Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

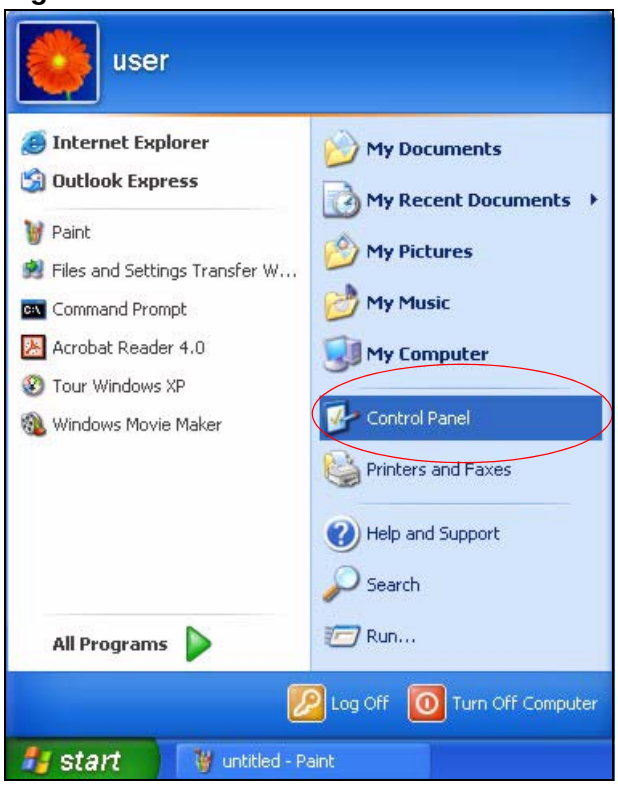
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

# Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 91** Windows XP: Start Menu

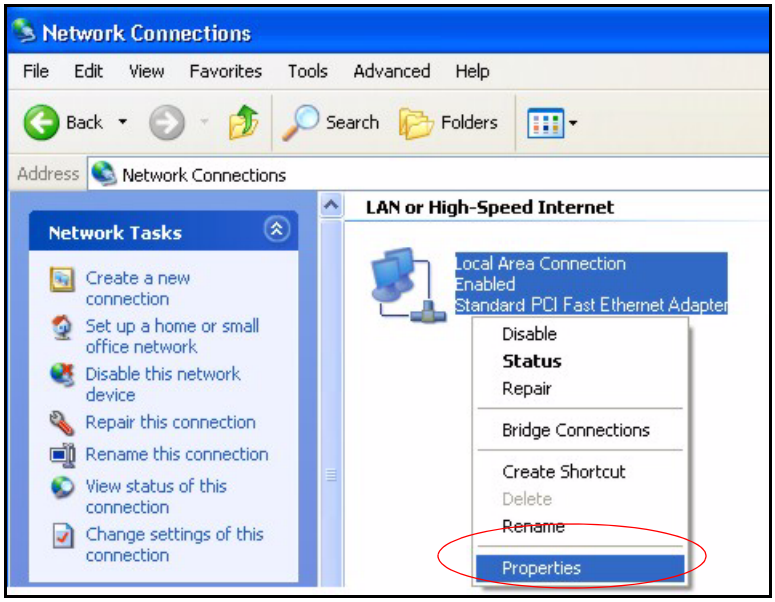



2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

**Figure 92** Windows XP: Control Panel

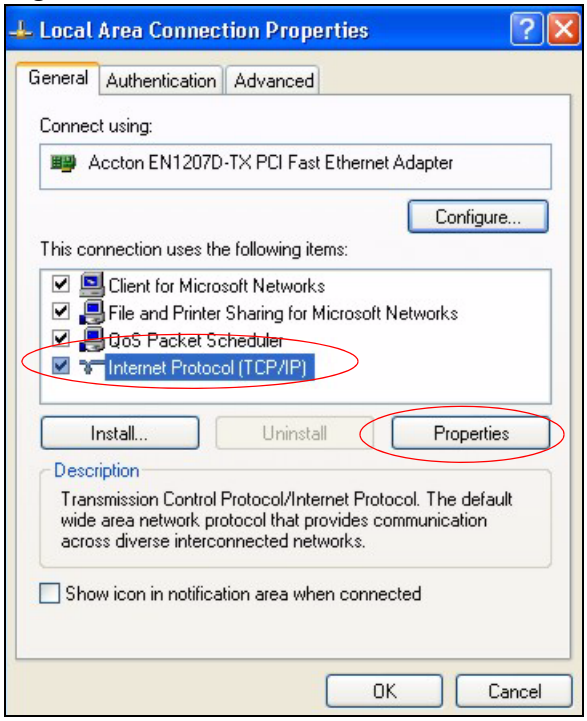
3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 93** Windows XP: Control Panel: Network Connections: Properties




4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

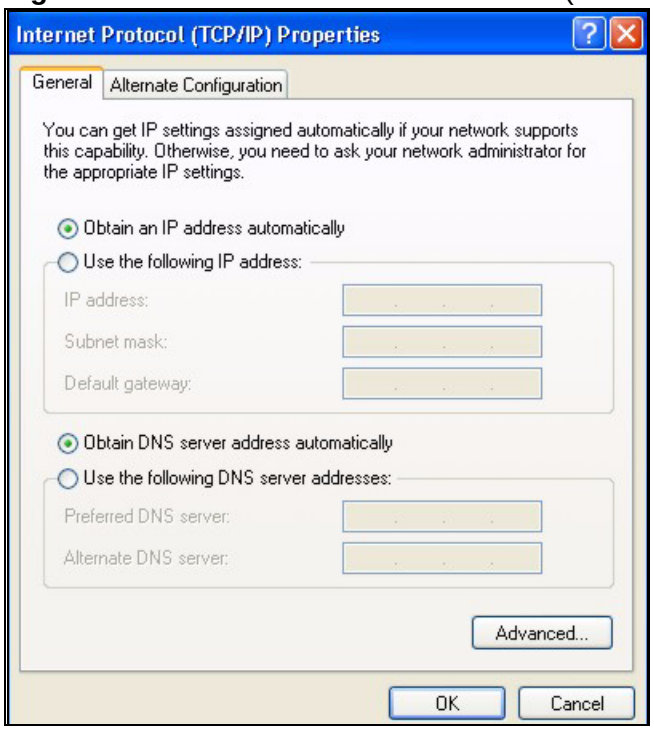
**Figure 94** Windows XP: Local Area Connection Properties




5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

**Figure 95** Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

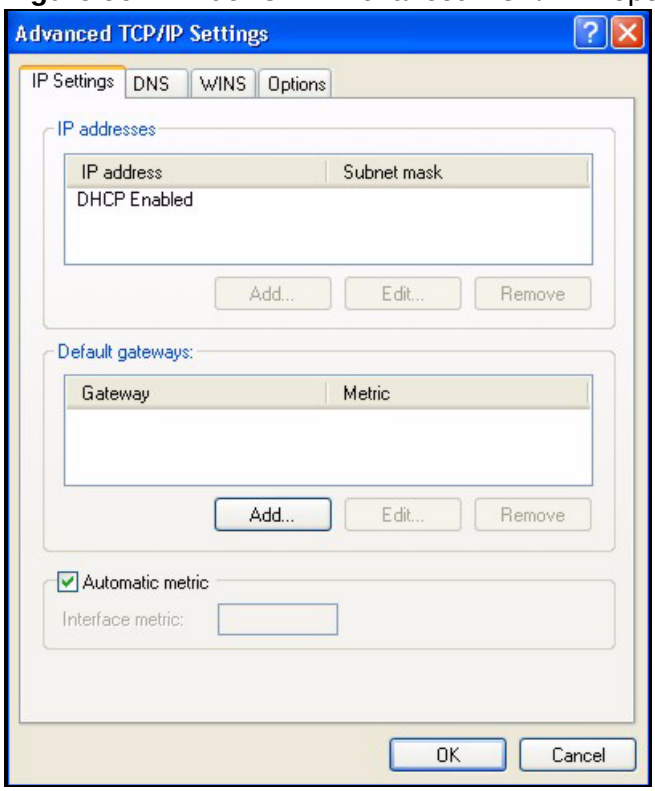
6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

**Figure 96** Windows XP: Advanced TCP/IP Properties

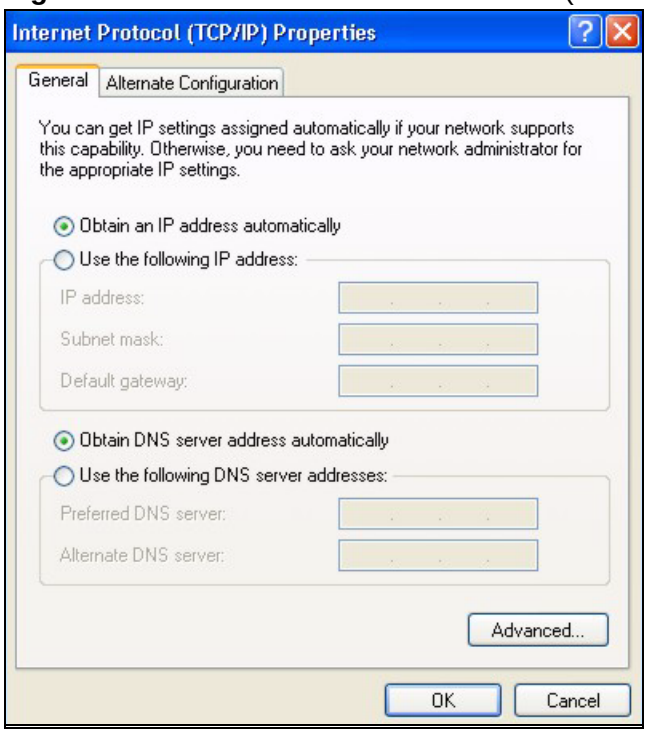



7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 97** Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your P-660H-T1v3s and restart your computer (if prompted).

### Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.

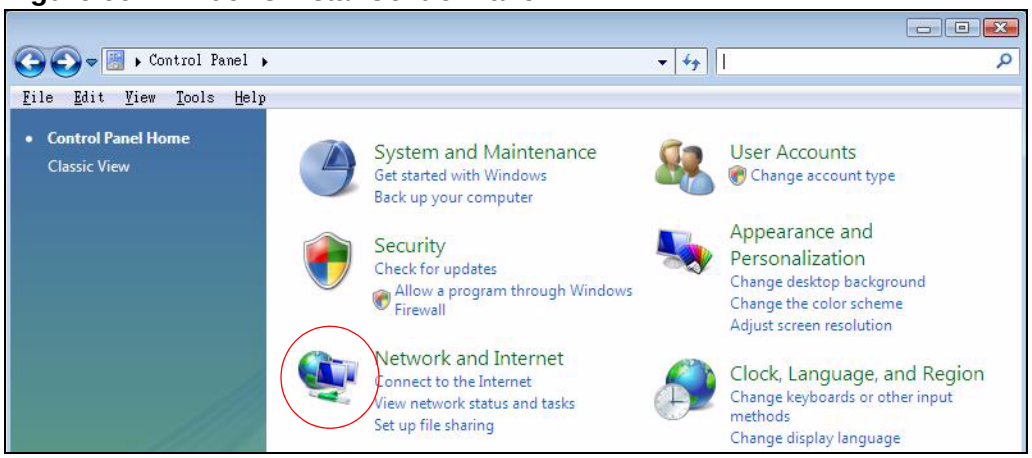
1 Click the **Start** icon, **Control Panel**.

**Figure 98** Windows Vista: Start Menu

Dr.eye 7.0 Professional
Media Player Classic
All Programs
Start Search
Connect To
Control Panel
Default Programs
Help and Support
Customize the appearance and functionality of your computer, add or remove programs, and set up network connections and user accounts.

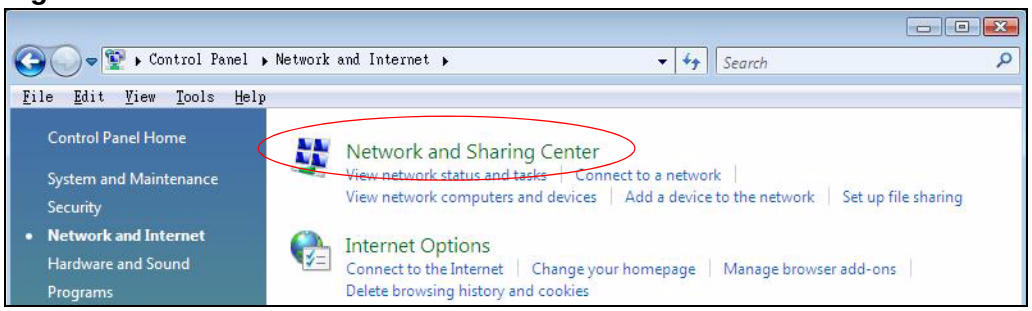
2 In the **Control Panel**, double-click **Network and Internet**.

**Figure 99** Windows Vista: Control Panel



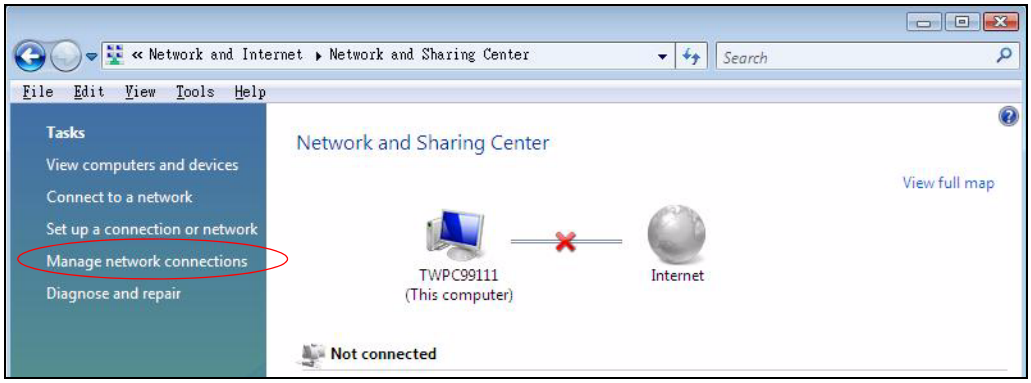

3 Click **Network and Sharing Center**.

**Figure 100** Windows Vista: Network And Internet



4 Click **Manage network connections**.

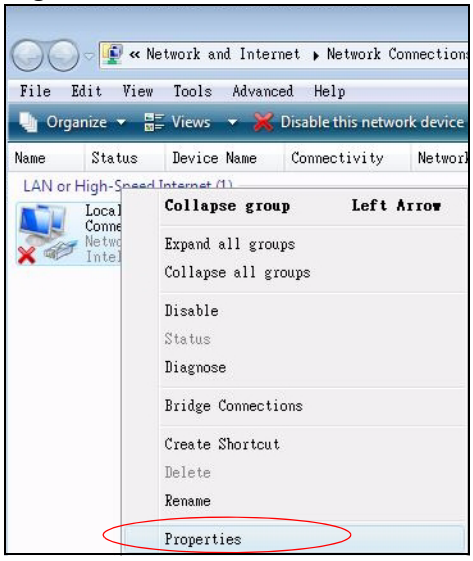
**Figure 101** Windows Vista: Network and Sharing Center




5 Right-click **Local Area Connection** and then click **Properties**.

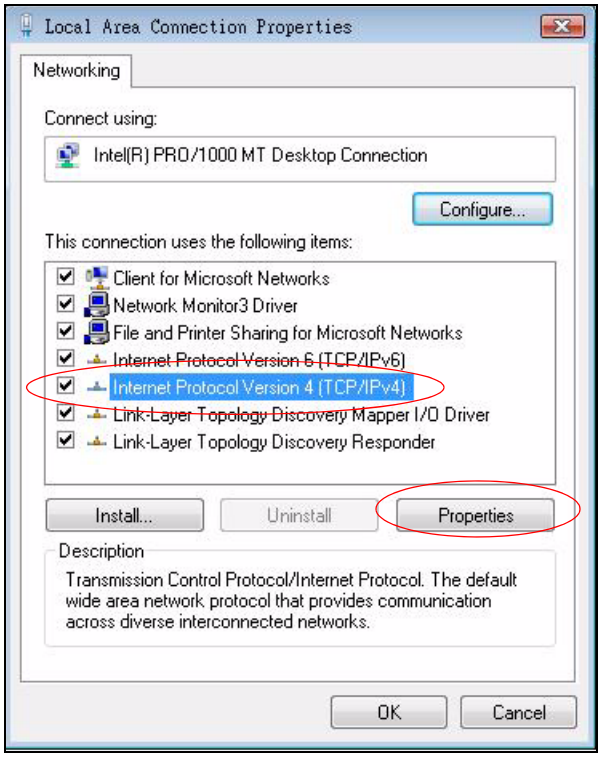
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

**Figure 102** Windows Vista: Network and Sharing Center



6 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

**Figure 103** Windows Vista: Local Area Connection Properties

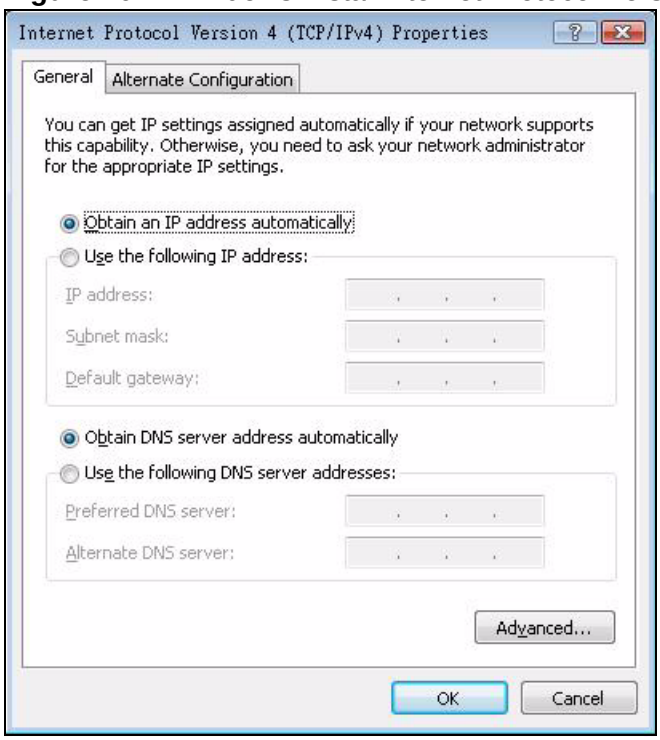



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General tab**).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

**Figure 104** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

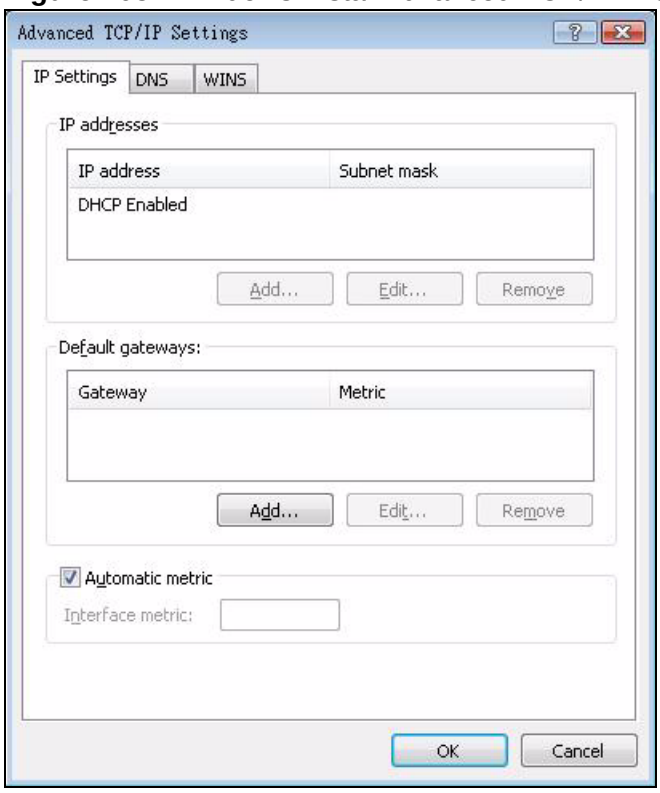
8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

**Figure 105** Windows Vista: Advanced TCP/IP Properties

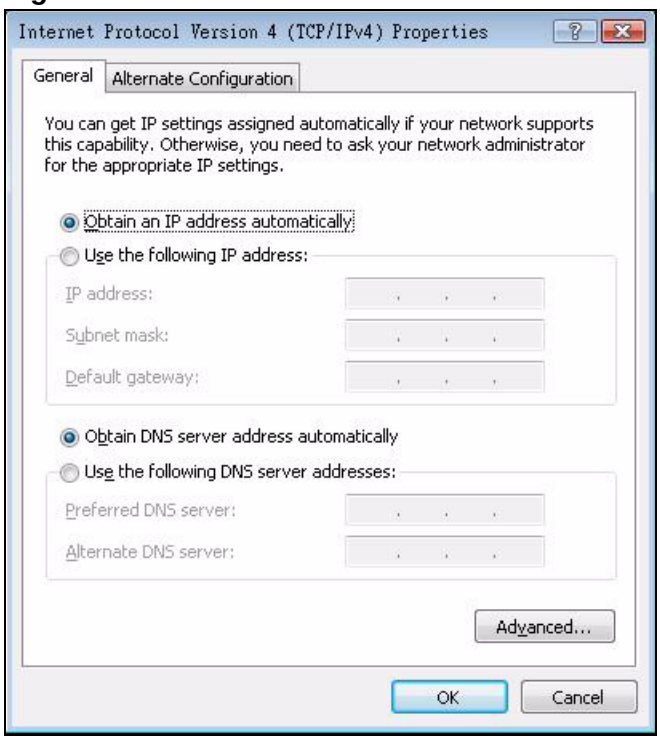



9 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General tab**):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 106** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

11 Click **Close** to close the **Local Area Connection Properties** window.

12 Close the **Network Connections** window.

13 Turn on your P-660H-T1v3s and restart your computer (if prompted).

## Verifying Settings

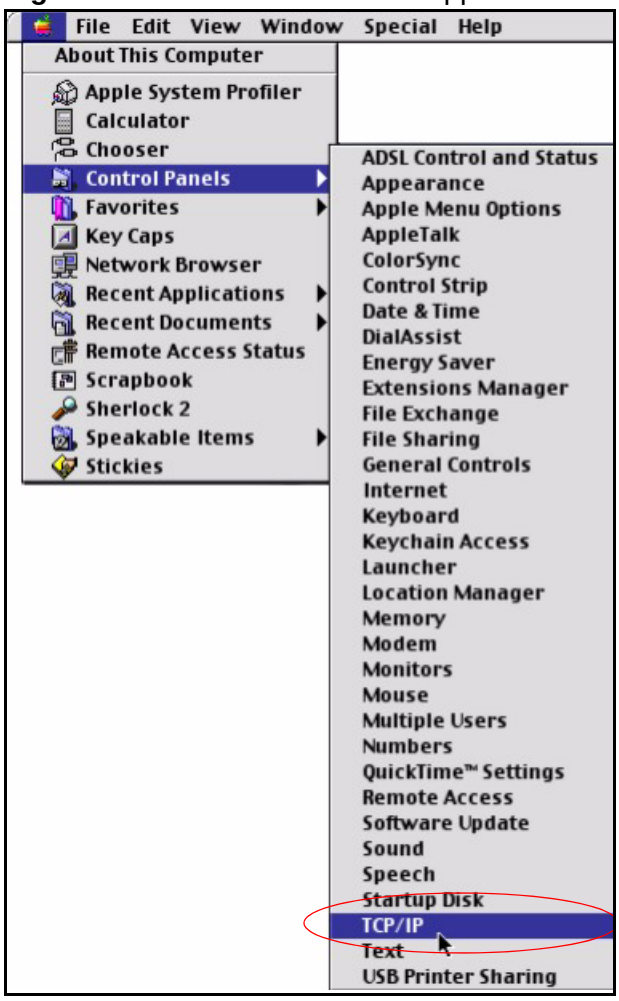
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

# Macintosh OS 8/9

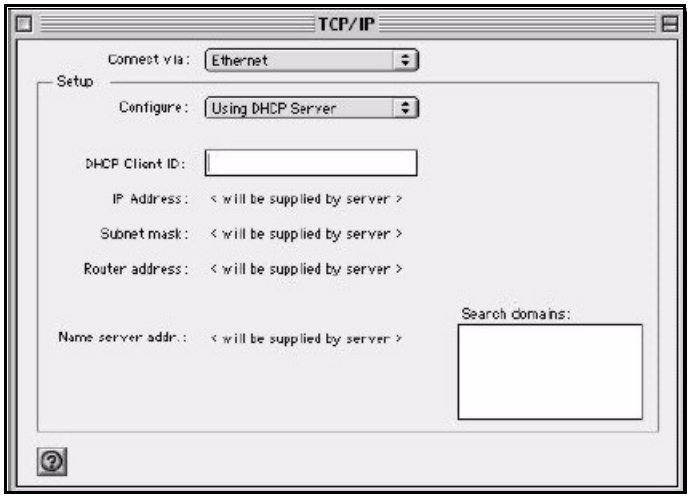
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 107** Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

**Figure 108** Macintosh OS 8/9: TCP/IP




3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your P-660H-T1v3s in the **Router address** box.

5 Close the **TCP / IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your P-660H-T1v3s and restart your computer (if prompted).

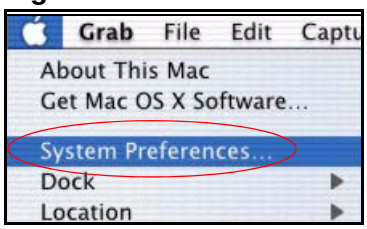
## Verifying Settings

Check your TCP/IP properties in the **TCP / IP Control Panel** window.

# Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 109** Macintosh OS X: Apple Menu

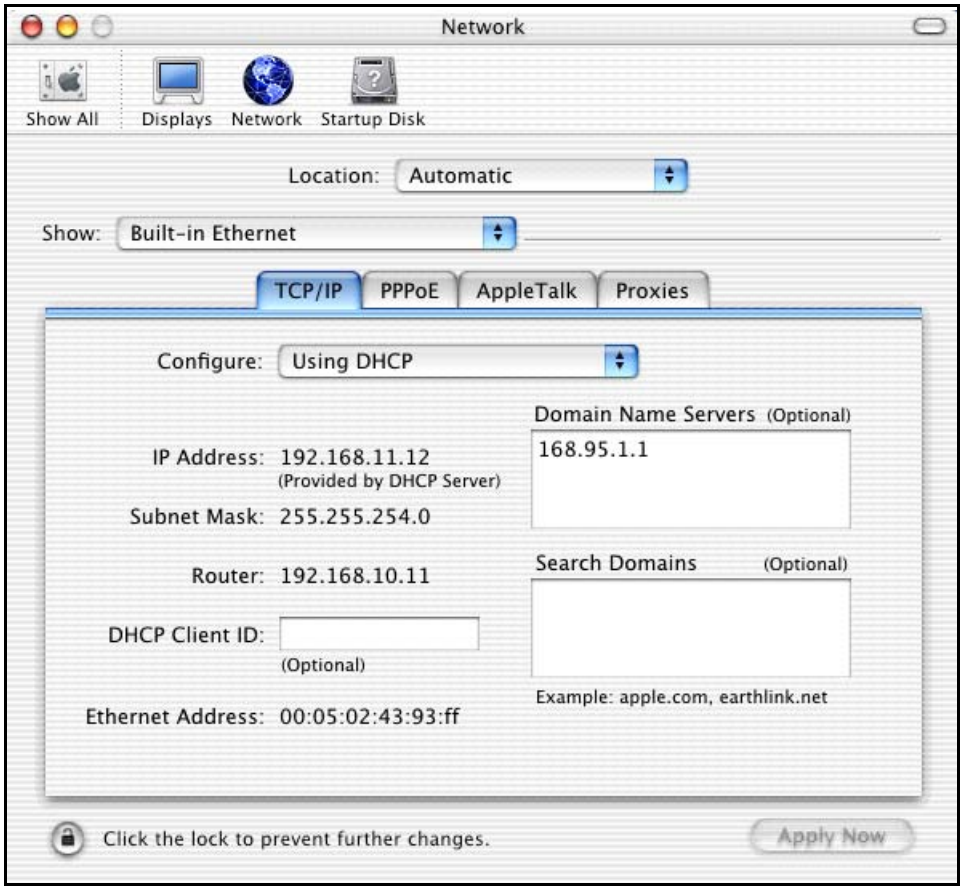



2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 110** Macintosh OS X: Network




4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your P-660H-T1v3s in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your P-660H-T1v3s and restart your computer (if prompted).

### Verifying Settings

Check your TCP/IP properties in the **Network** window.

## Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

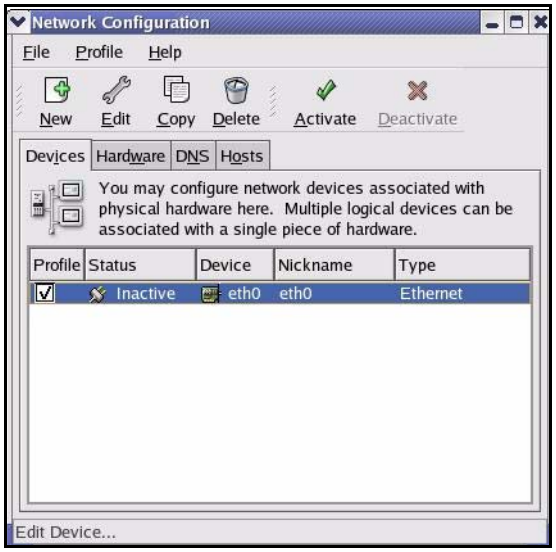
Note: Make sure you are logged in as the root administrator.

### Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 111** Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

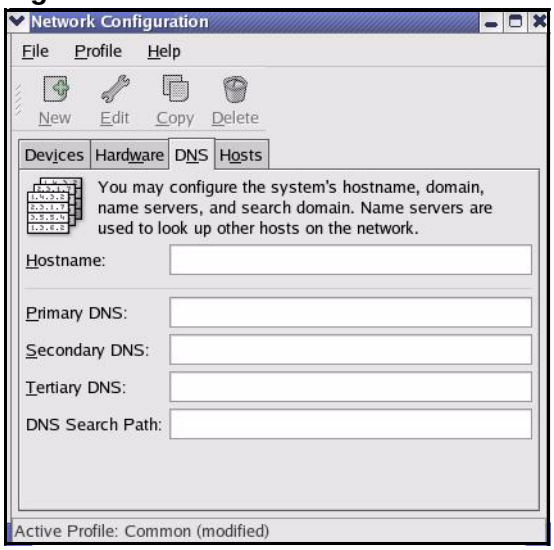
**Figure 112** Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

**Figure 113** Red Hat 9.0: KDE: Network Configuration: DNS




5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

**Figure 114** Red Hat 9.0: KDE: Network Configuration: Activate

Question
redhat-config-network:
You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.
Do you want to continue?
No
Yes

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

## Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 115** Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 116** Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the resolv.conf file in the /etc directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 117** Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter ./network restart in the /etc/rc.d/init.d directory. The following figure shows an example.

**Figure 118** Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

## Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 119** Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

# B

# Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

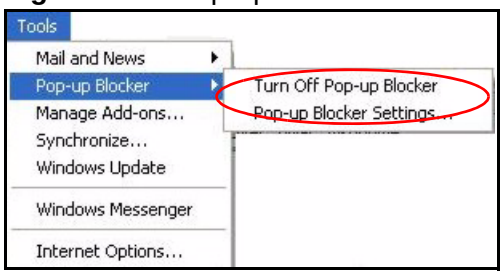
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

### Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 120** Pop-up Blocker

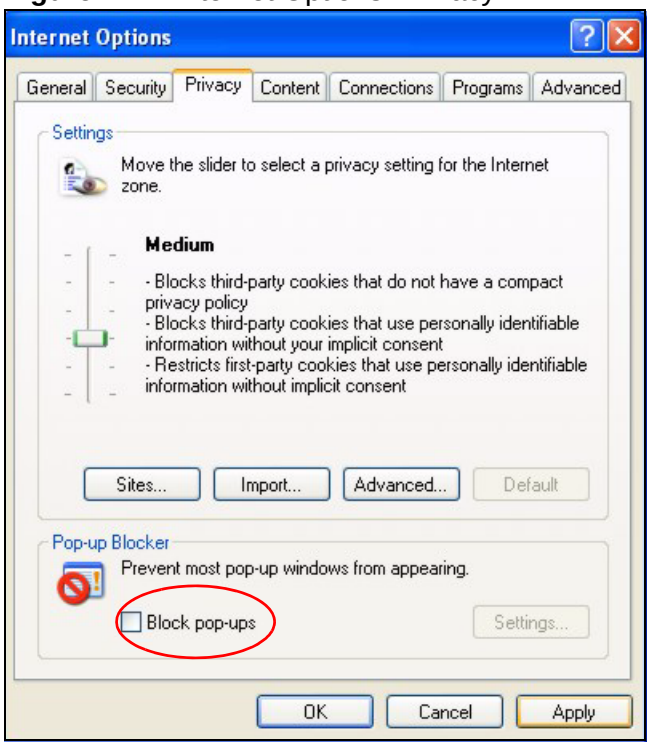



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 121** Internet Options: Privacy




3 Click **Apply** to save this setting.

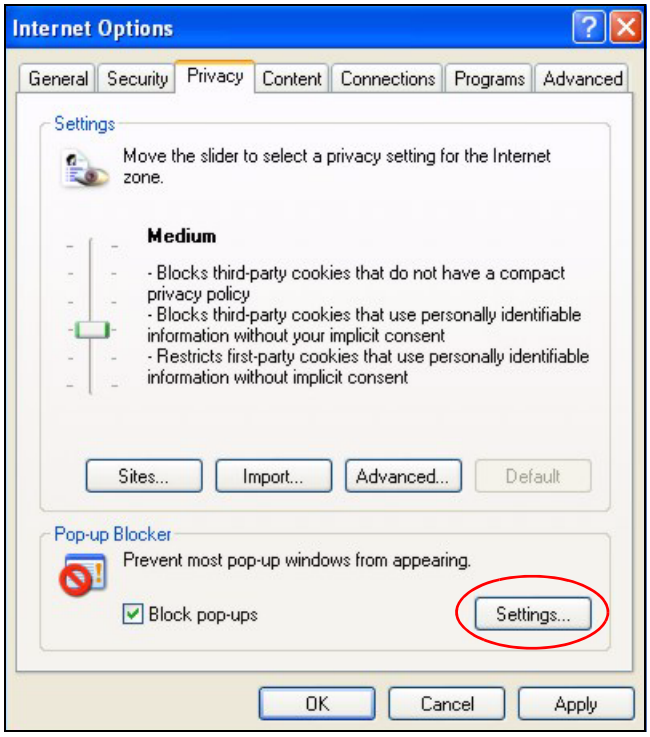
## Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

**Figure 122** Internet Options: Privacy




3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 123** Pop-up Blocker Settings

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

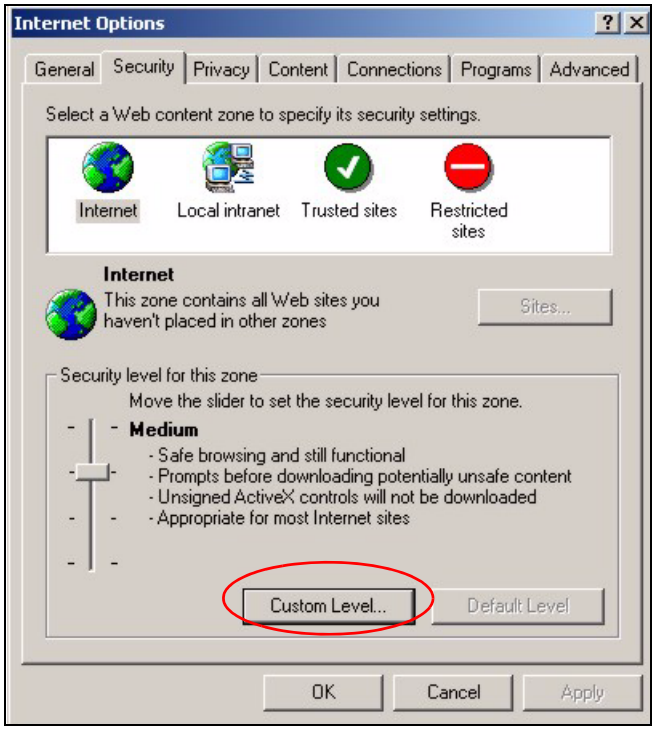
6 Click **Apply** to save this setting.

# JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

**Figure 124** Internet Options: Security




2 Click the **Custom Level...** button.

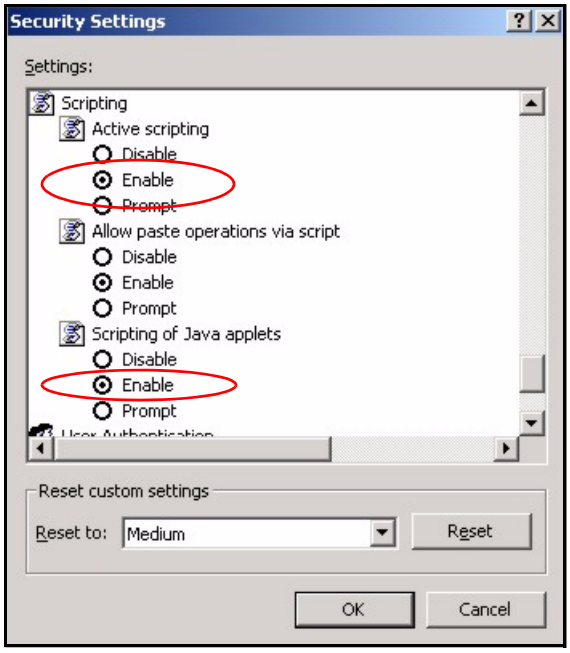
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

**Figure 125** Security Settings - Java Scripting




## Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

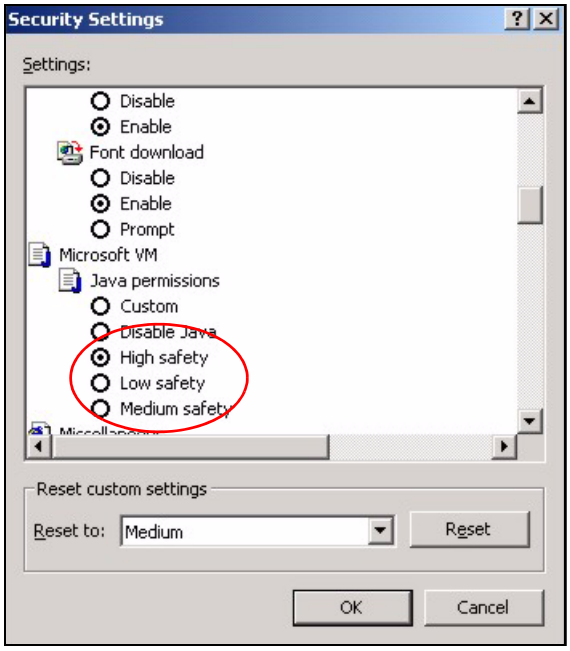
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

**Figure 126** Security Settings - Java



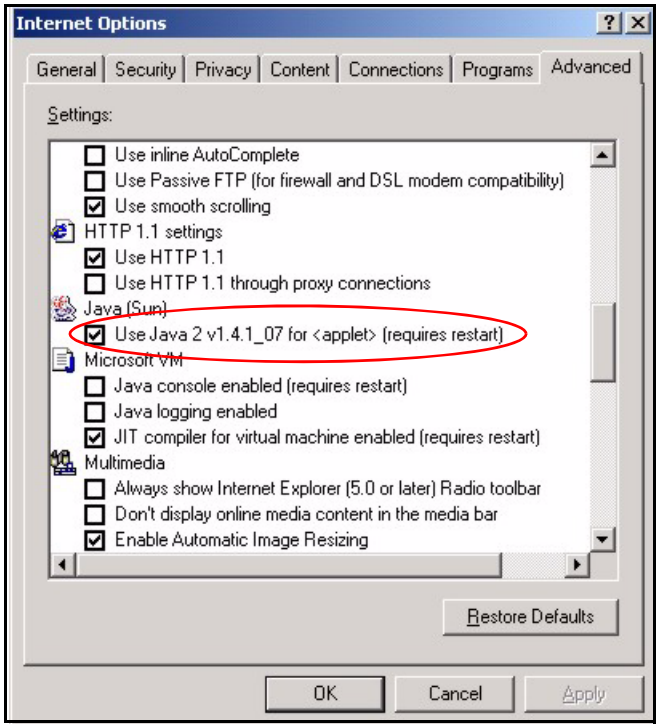

## JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

**Figure 127** Java (Sun)

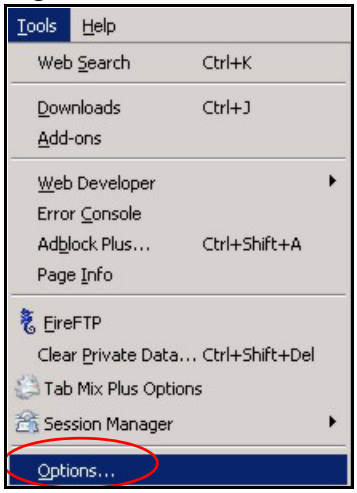



# Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

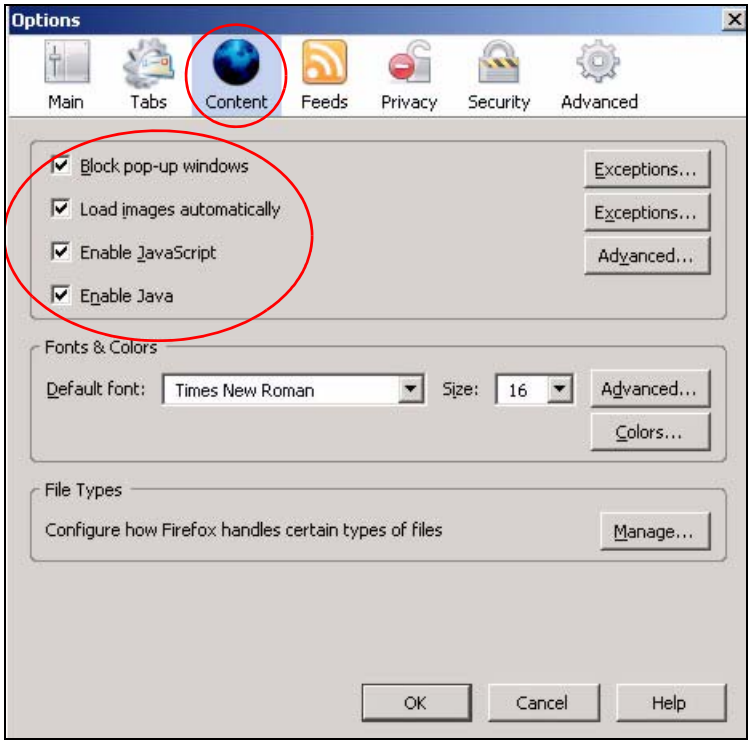
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

**Figure 128** Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

**Figure 129** Mozilla Firefox Content Security



C

# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

## Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

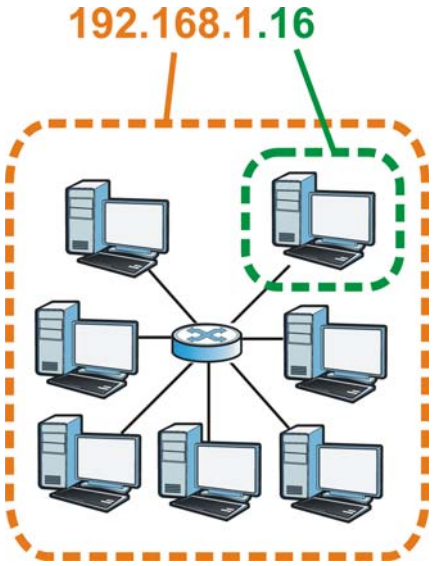
## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 130** Network Number and Host ID




How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 64** Subnet Masks

| | 1ST OCTET: (192) | 2ND OCTET: (168) | 3RD OCTET: (1) | 4TH OCTET (2) |
|---|---|---|---|---|
| IP Address (Binary) | 11000000 | 10101000 | 00000001 | 00000010 |
| Subnet Mask (Binary) | **11111111** | **11111111** | **11111111** | 00000000 |
| Network Number | **11000000** | **10101000** | **00000001** | |
| Host ID | | | | 00000010 |

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 65** Subnet Masks

| | BINARY | | | | DECIMAL |
|---|---|---|---|---|---|
| | 1ST OCTET | 2ND OCTET | 3RD OCTET | 4TH OCTET | |
| 8-bit mask | 11111111 | 00000000 | 00000000 | 00000000 | 255.0.0.0 |
| 16-bit mask | 11111111 | 11111111 | 00000000 | 00000000 | 255.255.0.0 |
| 24-bit mask | 11111111 | 11111111 | 11111111 | 00000000 | 255.255.255.0 |
| 29-bit mask | 11111111 | 11111111 | 11111111 | 11111000 | 255.255.255.248 |

## Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 66** Maximum Host Numbers

| SUBNET MASK | | HOST ID SIZE | | MAXIMUM NUMBER OF HOSTS |
|---|---|---|---|---|
| 8 bits | 255.0.0.0 | 24 bits | $2^{24} – 2$ | 16777214 |
| 16 bits | 255.255.0.0 | 16 bits | $2^{16} – 2$ | 65534 |
| 24 bits | 255.255.255.0 | 8 bits | $2^{8} – 2$ | 254 |
| 29 bits | 255.255.255.248 | 3 bits | $2^{3} – 2$ | 6 |

# Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 67** Alternative Subnet Mask Notation

| SUBNET MASK | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|---|---|---|---|
| 255.255.255.0 | /24 | 0000 0000 | 0 |
| 255.255.255.128 | /25 | 1000 0000 | 128 |
| 255.255.255.192 | /26 | 1100 0000 | 192 |
| 255.255.255.224 | /27 | 1110 0000 | 224 |
| 255.255.255.240 | /28 | 1111 0000 | 240 |
| 255.255.255.248 | /29 | 1111 1000 | 248 |
| 255.255.255.252 | /30 | 1111 1100 | 252 |

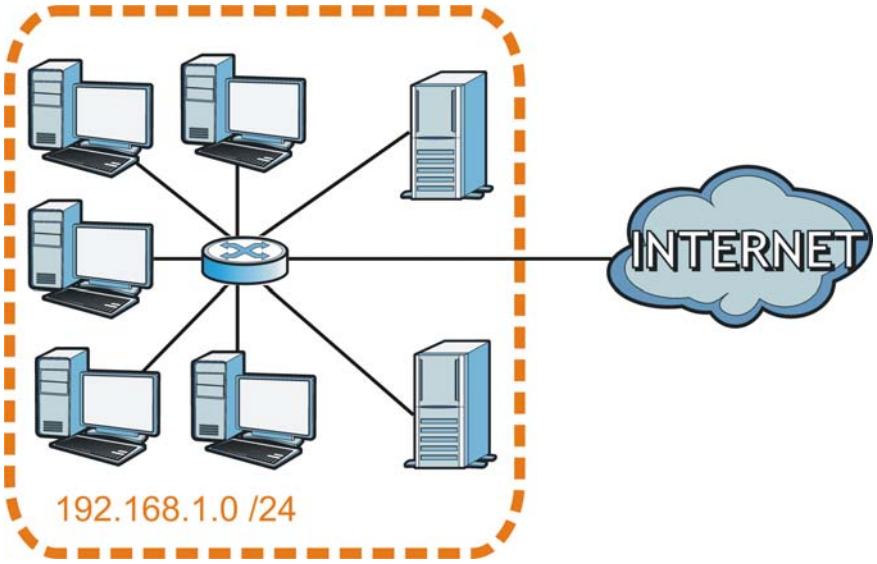
# Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8$ – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

**Figure 131** Subnetting Example: Before Subnetting

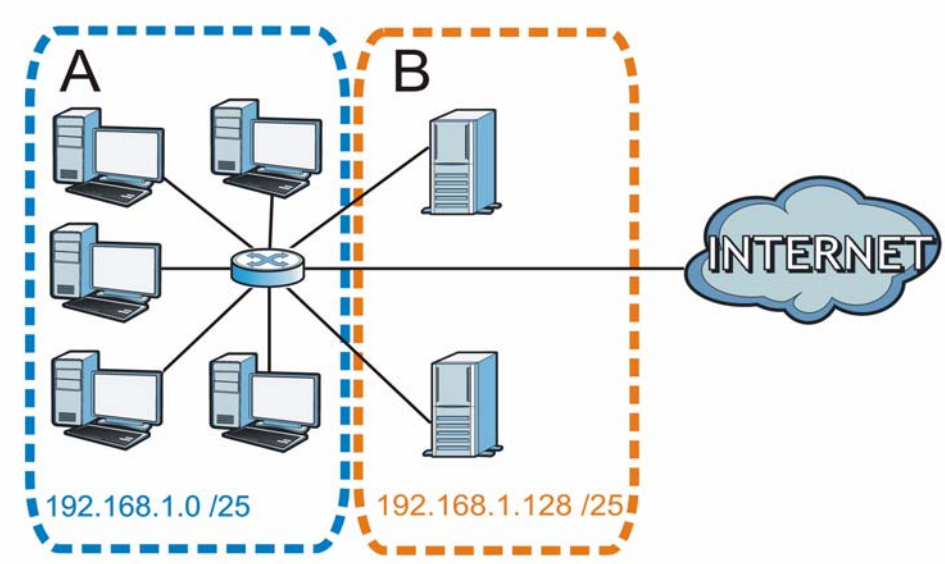



You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 132** Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6$ - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 68** Subnet 1

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address (Decimal) | 192.168.1. | 0 |
| IP Address (Binary) | 11000000.10101000.00000001. | **00**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.0 | Lowest Host ID: 192.168.1.1 | |
| Broadcast Address: 192.168.1.63 | Highest Host ID: 192.168.1.62 | |

**Table 69** Subnet 2

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 64 |
| IP Address (Binary) | 11000000.10101000.00000001. | **01**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.64 | Lowest Host ID: 192.168.1.65 | |
| Broadcast Address: 192.168.1.127 | Highest Host ID: 192.168.1.126 | |

**Table 70** Subnet 3

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 128 |
| IP Address (Binary) | 11000000.10101000.00000001. | **10**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.128 | Lowest Host ID: 192.168.1.129 | |
| Broadcast Address: 192.168.1.191 | Highest Host ID: 192.168.1.190 | |

**Table 71** Subnet 4

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 192 |
| IP Address (Binary) | 11000000.10101000.00000001. | **11**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.192 | Lowest Host ID: 192.168.1.193 | |
| Broadcast Address: 192.168.1.255 | Highest Host ID: 192.168.1.254 | |

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 72** Eight Subnets

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|---|---|---|---|---|
| 1 | 0 | 1 | 30 | 31 |
| 2 | 32 | 33 | 62 | 63 |
| 3 | 64 | 65 | 94 | 95 |
| 4 | 96 | 97 | 126 | 127 |
| 5 | 128 | 129 | 158 | 159 |
| 6 | 160 | 161 | 190 | 191 |
| 7 | 192 | 193 | 222 | 223 |
| 8 | 224 | 225 | 254 | 255 |

# Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 73** 24-bit Network Number Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.255.128 (/25) | 2 | 126 |
| 2 | 255.255.255.192 (/26) | 4 | 62 |
| 3 | 255.255.255.224 (/27) | 8 | 30 |
| 4 | 255.255.255.240 (/28) | 16 | 14 |
| 5 | 255.255.255.248 (/29) | 32 | 6 |
| 6 | 255.255.255.252 (/30) | 64 | 2 |
| 7 | 255.255.255.254 (/31) | 128 | 1 |

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 74** 16-bit Network Number Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.128.0 (/17) | 2 | 32766 |
| 2 | 255.255.192.0 (/18) | 4 | 16382 |
| 3 | 255.255.224.0 (/19) | 8 | 8190 |
| 4 | 255.255.240.0 (/20) | 16 | 4094 |
| 5 | 255.255.248.0 (/21) | 32 | 2046 |
| 6 | 255.255.252.0 (/22) | 64 | 1022 |
| 7 | 255.255.254.0 (/23) | 128 | 510 |
| 8 | 255.255.255.0 (/24) | 256 | 254 |
| 9 | 255.255.255.128 (/25) | 512 | 126 |
| 10 | 255.255.255.192 (/26) | 1024 | 62 |
| 11 | 255.255.255.224 (/27) | 2048 | 30 |
| 12 | 255.255.255.240 (/28) | 4096 | 14 |
| 13 | 255.255.255.248 (/29) | 8192 | 6 |
| 14 | 255.255.255.252 (/30) | 16384 | 2 |
| 15 | 255.255.255.254 (/31) | 32768 | 1 |

# Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP

addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the P-660H-T1v3s.

Once you have decided on the network number, pick an IP address for your P-660H-T1v3s that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your P-660H-T1v3s will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-660H-T1v3s unless you are instructed to do otherwise.

## Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

# D

# Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 75** Examples of Services

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| AH (IPSEC_TUNNEL) | User-Defined | 51 | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| AIM | TCP | 5190 | AOL's Internet Messenger service. |
| AUTH | TCP | 113 | Authentication protocol used by some servers. |
| BGP | TCP | 179 | Border Gateway Protocol. |
| BOOTP_CLIENT | UDP | 68 | DHCP Client. |
| BOOTP_SERVER | UDP | 67 | DHCP Server. |
| CU-SEEME | TCP/UDP<br>TCP/UDP | 7648<br>24032 | A popular videoconferencing solution from White Pines Software. |
| DNS | TCP/UDP | 53 | Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers. |
| ESP (IPSEC_TUNNEL) | User-Defined | 50 | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| FINGER | TCP | 79 | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |
| FTP | TCP<br>TCP | 20<br>21 | File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |
| HTTP | TCP | 80 | Hyper Text Transfer Protocol - a client/server protocol for the world wide web. |
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IMAP4 | TCP | 143 | The Internet Message Access Protocol is used for e-mail. |
| IMAP4S | TCP | 993 | This is a more secure version of IMAP4 that runs over SSL. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |

**Table 75** Examples of Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NetBIOS | TCP/UDP<br>TCP/UDP<br>TCP/UDP<br>TCP/UDP | 137<br>138<br>139<br>445 | The Network Basic Input/Output System is used for communication between computers in a LAN. |
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |
| NFS | UDP | 2049 | Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments. |
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| POP3S | TCP | 995 | This is a more secure version of POP3 that runs over SSL. |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| ROADRUNNER | TCP/UDP | 1026 | This is an ISP that provides services mainly for cable modems. |
| RTELNET | TCP | 107 | Remote Telnet. |
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |

**Table 75** Examples of Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| SFTP | TCP | 115 | The Simple File Transfer Protocol is an old way of transferring files between computers. |
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SMTPS | TCP | 465 | This is a more secure version of SMTP that runs over SSL. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |
| SQL-NET | TCP | 1521 | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSDP | UDP | 1900 | The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP). |
| SSH | TCP/UDP | 22 | Secure Shell Remote Login Program. |
| STRM WORKS | UDP | 1558 | Stream Works Protocol. |
| SYSLOG | UDP | 514 | Syslog allows you to send system logs to a UNIX server. |
| TACACS | UDP | 49 | Login Host Protocol used for (Terminal Access Controller Access Control System). |
| TELNET | TCP | 23 | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |
| TFTP | UDP | 69 | Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). |
| VDOLIVE | TCP<br>UDP | 7000<br>user-defined | A videoconferencing solution. The UDP port number is specified in the application. |

E

# Legal Information

## Copyright

Copyright © 2009 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

### Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

### Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Increase the separation between the equipment and the receiver.
2. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
3. Consult the dealer or an experienced radio/TV technician for help.

### Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or

materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

### Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

# Index

## Numerics

802.1p 145, 146
802.1Q/1P 135
  activation 137
  group settings 138
  port settings 140
  priority 135
  PVC 136
  PVID 140
  tagging frames 136, 139

## A

activation
  802.1Q/1P 137
  dynamic DNS 150
  DYNDNS wildcard 150
  firewalls 123
  NAT 107
  port forwarding 111
  QoS 143, 144
  SIP ALG 115
  SPI 123
  UPnP 163
address mapping 112
  rules 114
  types 113, 114, 118
Address Resolution Protocol, see ARP
administrator password 28, 172
alerts 177
alternative subnet mask notation 248
Any IP 102
  ARP 103
  example 102
application filter 127
applications, NAT 118
ARP 103
Asynchronous Transfer Mode, see ATM
ATM 195
  MBS 76, 82
  PCR 76, 81
  QoS 76, 81, 86
  SCR 76, 81
  status 195

## B

backup
  configuration 184, 185, 190
broadcast 70

## C

CBR 76, 81, 86
certifications 259
  notices 260
  viewing 260
CLI 21
client list 94
Command Line Interface, see CLI
configuration 189
  backup 184, 185, 190
  DHCP 93
  file 180
  firewalls 123
  IP alias 96
  IP precedence 144
  IP/MAC filter 129
  port forwarding 109
  reset 192
  restoring 181, 190
  static route 133
  WAN 71
  wizard 60
connection
  nailed-up 80, 84
  on demand 80
copyright 259

## D


DDoS 122
default server, NAT 108, 110
Denials of Service, see DoS
DHCP 90, 93, 98, 171
diagnostic 193
DiffServ Code Point, see DSCP
disclaimer 259
DNS 90, 93, 99, 157
Domain Name System, see DNS
DoS 122
DSCP 144
DSL connections, status 196
dynamic DNS 149
  activation 150
  wildcard 149
    activation 150
Dynamic Host Configuration Protocol, see DHCP
DYNDNS wildcard 149
  activation 150


## E


encapsulation 70, 73, 79
  ENET ENCAP 82
  PPPoA 83
  PPPoE 82
  RFC 1483 83
ENET ENCAP 73, 79, 82


## F


FCC interference statement 259
filters 125
  application 127
  IP/MAC 128
    structure 125
  IP/MAC filter
    configuration 129
  URL 125, 126
firewalls 121
  configuration 123
  DDoS 122
  DoS 122
  LAND attack 122
  Ping of Death 122
  status 35
  SYN attack 121
firmware 180, 187
  upgrading 182
  version 34
forwarding ports 106, 108
  activation 111
  configuration 109
  example 109
  rules 111
FTP 21, 155
  backing up configuration 184
  limitations 181
  restoring configuration 181, 182
  upgrading firmware 182, 183


## I


IANA 253
  Internet Assigned Numbers Authority
    see IANA
ICMP 158
IGA 116
IGMP 70, 90, 92, 101
ILA 116
Inside Global Address, see IGA
Inside Local Address, see ILA
Internet Group Multicast Protocol, see IGMP
IP address 70, 74, 80, 84, 90, 99
  ARP 103
  default server 108, 110
  ping 193
  private 100
IP alias 96
  configuration 96
  NAT applications 118
IP precedence 145, 147
  configuration 144
IP/MAC filter 128
  configuration 129
  structure 125

## L


LAN 89
  Any IP 102
    example 102
  client list 94
  DHCP 90, 93, 98
  DNS 90, 93, 99
  IGMP 90, 101
  IP address 90, 91, 99
  IP alias 96
    configuration 96
  MAC address 95
  multicast 90, 92, 101
  RIP 90, 92, 97, 101
  status 34
  subnet mask 90, 91, 99
LAND attack 122
limitations
  FTP 181
Local Area Network, see LAN
login 27
  passwords 27, 28
logs 177
  alerts 177


## M


MAC address 95
mapping address 112
  rules 114
  types 113, 114, 118
Maximum Burst Size, see MBS
Maximum Transmission Unit, see MTU
MBS 76, 82, 85
MTU 76, 82
multicast 70, 76, 81, 90, 92, 101
  IGMPInternet Group Multicast Protocol, see IGMP
multiplexing 73, 79, 83
  LLC-based 84
  VC-based 83


## N


nailed-up connection 74, 80, 84
NAT 80, 105, 106, 116, 253
  activation 107
  address mapping 112
    rules 114
    types 113, 114, 118
  applications 118
    IP alias 118
  default server IP address 108, 110
  example 117
  global 116
  IGA 116
  ILA 116
  inside 116
  local 116
  outside 116
  P2P 107
  port forwarding 106, 108
    activation 111
    configuration 109
    example 109
    rules 111
  remote management 153
  SIP ALG 115
    activation 115
  SUA 106, 107
Network Address Translation
  see NAT
Network Address Translation, see NAT


## P


P2P 107
passwords 27, 28
  administrator 172
PCR 76, 81, 85
Peak Cell Rate, see PCR
Ping of Death 122
port forwarding 106, 108
  activation 111
  configuration 109
  example 109
  rules 111
PPPoA 73, 79, 83

PPPoE 73, 79, 82
private IP address 100
product registration 261
PVC 136
PVID 140

## Q

QoS 141
  802.1p 145, 146
  activation 143, 144
  DSCP 144
  example 141
  IP precedence 145, 147
  priority queue 147
Quality of Service, see QoS

## R

registration
  product 261
related documentation 3
remote management 151
  DNS 157
  FTP 155
  ICMP 158
  limitations 152
  NAT 153
  Telnet 154
  WWW 153
reset 24, 192
restart 192
restoring configuration 181, 190
restrictions
  FTP 181
RFC 1483 73, 79, 83
RIP 75, 81, 90, 92, 97, 101
Routing Information Protocol, see RIP
rules, port forwarding 111

## S

safety warnings 7
SCR 76, 81, 85
Security Parameter Index, see SPI
setup 189
  DHCP 93
  firewalls 123
  IP alias 96
  IP precedenceQoS
    IP precedence 144
  IP/MAC filter 129
  port forwarding 109
  static route 133
  WAN 71
  wizard 60
shaping traffic 85, 86
Single User Account, see SUA
SIP ALG 115
  activation 115
SPI 122
  activation 123
static route 131
  configuration 133
  example 131
status 30, 33, 35
  ATM 195
  DSL connections 196
  firewalls 35
  firmware version 34
  LAN 34
  WAN 34
SUA 106, 107
subnet 245
subnet mask 90, 99, 246
subnetting 248
Sustain Cell Rate, see SCR
SYN attack 121
syntax conventions 5
system 172
  backing up configuration 185
  backup configuration 184
  firmware 180, 187
    upgrading 182
    version 34
  passwords 27, 28
    administrator 172

reset 24
restoring configuration 181
status 30, 33
firewalls 35
LAN 34
WAN 34
time 173


## T


tagging frames 136, 139
Telnet 154
TFTP 185
backing up configuration 185
upgrading firmware 183
time 173
TR-069 21
trademarks 259
traffic priority 135
traffic shaping 85
example 86


## U


UBR 76, 81, 87
unicast 70
Universal Plug and Play, see UPnP
upgrading firmware 182, 187
UPnP 161
activation 163
cautions 162
NAT traversal 161
URL 125
URL filter 126
URL 125


## V


VBR 86
VBR-nRT 76, 81, 86
VBR-RT 76, 81, 86
VCI 73, 79, 84
Virtual Channel Identifier, see VCI
Virtual Local Area Network, see VLAN
Virtual Path Identifier, see VPI
VLAN 135
802.1P priority 135
activation 137
group settings 138
port settings 140
PVC 136
PVID 140
tagging frames 136, 139
VPI 73, 79, 84


## W


WAN 69
ATM QoS 76, 81, 86
encapsulation 70, 73, 79
IGMP 70
IP address 70, 74, 80, 84
mode 72, 79
modulation 72
MTU 76, 82
multicast 70, 76, 81
multiplexing 73, 79, 83
nailed-up connection 74, 80, 84
NAT 80
RIP 75, 81
setup 71
status 34
traffic shaping 85
example 86
VCI 73, 79, 84
VPI 73, 79, 84
warranty 260
note 261
web configurator 21, 27
login 27
passwords 27, 28
Wide Area Network, see WAN
wizard 57
configuration 60